UNIVERSIDAD POLITÉCNICA DE MADRID

ESCUELA UNIVERSITARIA DE INGENIERÍA TÉCNICA DE TELECOMUNICACIÓN

PROYECTO FIN DE CARRERA

ESTUDIO DE LA TECNOLOGÍA IMS Y DISEÑO DE UNA SOLUCIÓN DE TELEFONÍA MULTIMEDIA

Bárbara Morata González

Septiembre de 2012

Agradecimientos

En primer lugar mis agradecimientos a **Miguel Serrano** por todo su apoyo tanto en la realización de este proyecto como profesionalmente en mi día a día en Ericsson. Agradezco además enormemente a Lola Villegas y a Moisés Barcessat su interés y la ayuda que siempre me ofrecen.

También quiero destacar mi muy especial agradecimiento a mi profesor y tutor, Alfonso Martín Marcos, por toda su comprensión, colaboración, interés y apoyo, no sólo durante la realización del PFC, sino también durante todos estos años en la escuela, los cuales nunca olvidaré.

Gracias a toda mi familia, en especial a mis hermanos y mis padres, por comprender y respetar mis horas de estudio además de demostrar su apoyo incondicional y su a veces 'excesiva' confianza en mí. A partir de ahora no tengo 'excusa' para faltar a un cumpleaños!

Gracias a todos los 'telekos' con los que he compartido tantos buenos momentos en la universidad, descansos de biblioteca, cafés…y etc! Siempre recordaré la EUITT.

A Laura Grijuela, por nuestro enorme trabajo en equipo a lo largo de la carrera…y nuestra gran amistad fuera de ella. Gracias por todo!

Gracias a Thais Ruiz, por su seguimiento tan cercano a mis 'proyectos'…y su grandísimo apoyo. Nada sería igual sin ti (L)

Para Eva Muñoz, por demostrar hasta dónde puede llegar la amistad. Gracias de todo corazón. Eres increíble.

Gracias Pablo, por haberme hecho ver la parte positiva cada día; y por soportar mis interesantes charlas *teen* …" *you're my wonderwall* ".

Y por último, este proyecto va dedicado a mi abuela, Rosario Alves, por ser una de las personas que sin duda más orgullosa se sienta de mi trabajo.

Abstract

The principal objective in this Final Degree Project is to provide an overview of the architect of the IMS Network, considering the behavior of nodes that integrate this network and the main functionalities that each of them implements.

During the study of this Project has taken into account that IMS network has turned Telecommunications world, due to the strong convergence of the services offered. This technology shows a wide range of multimedia applications, in enterprise as much as residential environment.

As a practical development a high-level design is presented. It involves the expansion of existing capacity for one of IMS network nodes for a national operator offering 'Business Trunking' service for enterprises.

The goal to achieve in this case is to analyze the impact caused by the inclusion of this new element in the rest of the nodes within the IMS network. To manage to prove the ease of the operator, in expanding the capacity of its network, and considering IMS technology allows to obtain several benefits for both supplier and end user.

Resumen

El objetivo fundamental del Proyecto Fin de Carrera es ofrecer una visión global de la arquitectura de red IMS ("*IP Multimedia Subsystem*") conociendo el comportamiento de los nodos que la forman y las funcionalidades que cada uno de ellos implementa.

Durante la realización del proyecto se ha tenido en cuenta que las redes IMS han transformando el sector de las telecomunicaciones debido a la gran convergencia de los servicios que ofrece. Esta tecnología presenta un amplio abanico a las aplicaciones multimedia, tanto en el entorno empresarial como residencial

Como desarrollo práctico se expone un diseño de alto nivel que consiste en la ampliación de la capacidad existente de uno de los nodos de la red IMS para un operador nacional ofreciendo el servicio '*Business Trunking*' para grandes clientes.

El objetivo destinado alcanzar con este caso práctico es el análisis del impacto que supone la inclusión de este nuevo elemento en el resto de nodos que forman la red. Consiguiendo demostrar la facilidad para el operador, a la hora de ampliar la capacidad de su red, sin olvidarnos que esto conlleva numerosos beneficios tanto a nivel de proveedor como de usuario final.

Índice de contenido

Índice de figuras

Índice de tablas

Lista de acrónimos y términos utilizados

ADSL	Asymmetric Digital Subscriber Line
AS	Application Server
AuC	Authentication Centre
BW	BandWidth. Ancho de banda.
CAPEX	CApital EXPenditures
CDMA	Code Division Multiple Access
CSCF	Call Service Control Function
DTMF	Dual Tone Multi-Frequency
ETSI	European Telecommunications Standards Institute
FE	Fast Ethernet
FQDN	Fully Qualified Domain Name
GSM	Global System for Mobile communications
HLR	Home Location Register
HSS	Home Subscriber Server
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISP	Internet Service Provider.
ITU	International Telecommunication Union
IU	Interfaz de Usuario
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NAT	Network Address Translation.
MGCF	Media Gateway Control Function
MGW	Media Gateway
MPLS	Multi Protocol Label Switching
MRF	Media Resource Function
OMA	Open Mobile Alliance
OPEX	Operating Expenditure
PABX	Private Automatic Branch Exchange
PBX	Private Branch Exchange
PoC	Push to Talk over Cellular
PSTN	Public Switched Telephone Network

PTT	Push to talk
RDSI	Red Digital de Servicios Integrados.
RFC	Request for Comments
RTB	Red Telefónica Básica
RTCP	Real time Transport Control Protocol
RTP	Real-time Transport Protocol
SG	Signalling Gateway
SIP	Session Initiation Protocol
SSO	Single Sign On
SNMP	Simple Network Management Protocol.
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
ToIP	Telefonía IP
UDP	User Datagram Protocol
VLAN	Virtual LAN.
VoIP	Voice over IP
VPN	Virtual Private Network.
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
XML	Extensible Markup Language
3GPP	Third Generation Partnership Project

1. Introducción

1.1. Objetivos y alcance del proyecto

En la actualidad, debido al gran avance de las TIC y la demanda por parte de los usuarios, los operadores de red llegan a la conclusión de no poder continuar creciendo ofreciendo simplemente llamadas de voz. Necesitan una manera de proveer más servicios para atraer a los usuarios, como Internet móvil mediante redes de conmutación de paquetes. Y así es como nace IMS, creando una plataforma común para desarrollar servicios multimedia para los usuarios finales y los mecanismos necesarios para tarificar el uso de las redes conmutadas de paquetes ofreciendo nuevos servicios.

Con esto, el objetivo principal de este Proyecto Fin de Carrera es exponer los rasgos principales de la arquitectura de red de esta tecnología, y desarrollar un diseño basado en la misma para un operador de red nacional. El alcance recoge los siguientes puntos:

- Describir las principales características de IMS así como las ventajas que ofrece.
- Describir los principales protocolos de señalización que se implementan en este tipo de redes.
- Estudiar los nodos que forman el estándar de arquitectura de red IMS y el funcionamiento de la misma.
- Exponer un diseño real de alto nivel de IMS para la implementación de determinadas funcionalidades dentro de la red de un operador nacional.
- Analizar las ventajas económicas que ofrece IMS a los operadores de red mediante una valoración real de costes.

1.2. Contenido y organización del proyecto

A continuación se describe brevemente el contenido de cada uno de los capítulos del proyecto:

- **Capítulo 1: Introducción**

En este capítulo se exponen las razones más relevantes que nos llevan a tratar IMS como tema de este proyecto. A su vez, se define el alcance y la organización del documento.

- **Capítulo 2: Introducción a IMS**

En este capítulo se exponen las principales ventajas que ofrece IMS y la evolución de las redes hacia la misma.

- **Capítulo 3: Estandarización de IMS**

Se expone de manera sintetizada las principales protocolos de IMS y que que se emplearán durante la implementación de cualquier red de estas características.

- **Capítulo 4: Protocolos principales**

Se expone de manera sintetizada las principales protocolos de IMS y que que se emplearán durante la implementación de cualquier red de estas características.

- **Capítulo 5: Arquitectura IMS**

En este capítulo se exponen los nodos que integran la red IMS, con sus principales funcionalidades e interfaces de comunicación hacia el resto de nodos, basándonos en el estándar 3GPP y TISPAN.

- **Capítulo 6: Registro y casos de tráfico**

Se valoran posibles escenarios dentro de la red IMS indicando el flujo de datos dentro de la misma dependiendo de la funcionalidad que se procese.

- **Capítulo 7: Caso práctico**

En este capítulo de lleva a cabo el diseño de alto nivel de una solución IMS para un operador nacional de comunicaciones basado en el estándar y la arquitectura

estudiada que quiere ampliar su capacidad de red para ofrecer servicios ‘Business Trunking’

- **Capítulo 8: Conclusiones y líneas futuras de trabajo**

En este capítulo se exponen las conclusiones obtenidas tras la elaboración del proyecto y se proponen las distintas posibles líneas de trabajo a las que da pie este documento.

- **Capítulo 9: Documentación**

Se detalla la bibliografía utilizada durante la realización del proyecto. Para las consultas web, se indicará su “url” correspondiente.

2. Introducción a IMS

Las redes de subsistema multimedia IP, IMS (IP Multimedia Subsystem) son la clave tecnológica para construir redes basadas en la tecnología IP de la manera más eficiente posible, ofreciendo una amplia gama de servicios y aplicaciones sobre la misma infraestructura IP con acceso independiente sobre redes fijas y móviles, reduciendo así considerablemente el coste al operador que proporciona el servicio.

IMS es imprescindible en la evolución de las redes anteriores a las redes basadas en IP, donde todo tipo de información puede ser transmitida en una sesión de red, como voz, texto, audio o vídeo. Además, favorece la creación de nuevos servicios, la convergencia y la interconexión de los mismos, basándose en un estándar abierto.

Para el usuario final, ofrece nuevas opciones de comunicación combinando sesiones de voz con elementos multimedia, como almacenar vídeo o jugar con otros usuarios de la red mientras se mantiene una llamada telefónica de voz, abriendo aún más las posibilidades de comunicación ya existentes. Además, permite aplicaciones atractivas para los usuarios como el servicio de 'presencia' para comprobar quién está disponible en un determinado momento o el intercambio de información en tiempo real.

2.1. Diferencias con las redes anteriores

Si comparamos la tecnología IMS con las utilizadas anteriormente, llegamos a la conclusión de que la principal diferencia es que IMS crea un entorno donde cualquier servicio puede acceder a cualquier aspecto de la sesión, permitiendo a los operadores ofrecer servicios más completos que los anteriores, donde cada servicio era independiente de los demás y se realizaban implementaciones de cada capa de funcionalidad separadas para cada servicio, duplicando la estructura por toda la red.

Cuando los servicios de una red acceden a todos los aspectos de una sesión, pueden realizar varias acciones simultáneamente, como por ejemplo cambiar el estado de presencia de un usuario, sin necesidad de enviar información mediante radio a otro terminal.

Otra de las principales ventajas es que IMS hace uso de las redes conmutadas de paquetes, que en general son más eficientes que las redes conmutadas de circuitos. De esta manera, la interoperabilidad con dispositivos que pueden tener acceso a estas redes es posible, como los ordenadores. Esto hace que aumente la cantidad de usuarios dispuestos a utilizar IMS, proporcionando tanto a los operadores fijos como móviles la convergencia fijo-móvil.

Los servicios IMS residen en los servidores de aplicación AS ("*Aplication Servers"*) y los sistemas son diseñados para soportar varias aplicaciones. La misma infraestructura se emplea para todos los servicios de la red. Cuando queremos implementar un nuevo servicio se utiliza toda la infraestructura ya creada, por lo que no hay que centrarse en procesos básicos ya implementados como la autenticación o la tarificación, y es posible dedicarse exclusivamente al propio servicio.

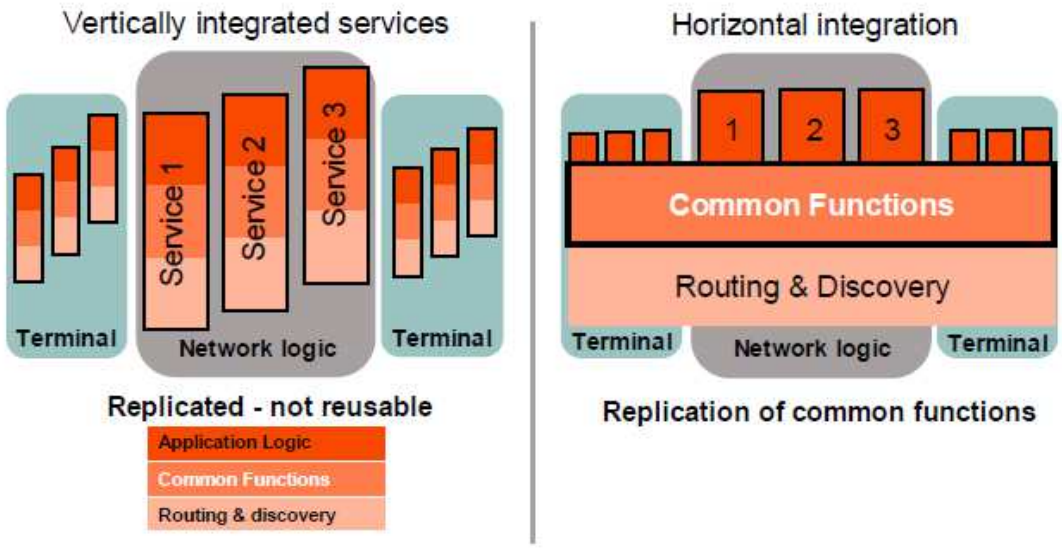


Figura 1. Integración horizontal de los servicios en IMS Figura 1

Sin embargo, en las redes que no sean IMS se soporta cada servicio de manera independiente, con sus propios nodos lógicos especializados en ese servicio. Cada uno de ellos se crea desde el inicio, incluyendo los aspectos básicos de la red. Este tipo de implementación es más compleja de construir y más costosa en cuanto al mantenimiento. Así IMS proporciona un conjunto de funciones comunes y genéricas a toda la estructura que se pueden reusar para cualquier nueva implementación o

servicio. Algunos ejemplos son la gestión de grupos o listas, el servicio de presencia, provisionamiento, operación y mantenimiento y tarificación, entre otros.

Además otra de las ventajas de IMS es que reduce el OPEX y CAPEX para los operadores, especialmente en provisionamiento, operación y mantenimiento y sistemas de facturación.

Para poder interactuar entre servicios distintos de la red, son necesarios protocolos de comunicación que permitan cada interacción. Este punto hace muy eficiente a las redes IMS, puesto que al implementar servicios sobre la misma infraestructura de red, basada en IP, emplea SIP, SDP y otros protocolos estándar de internet para la provisión de los servicios multimedia.

2.2. Evolución a las redes all-IP

En la actualidad, las redes evolucionan hacia las denominadas *all-IP*, basadas en su totalidad en el protocolo IP. Esta evolución se está llevando a cabo en pequeños pasos, hasta que los dispositivos, el acceso a la red y los servicios empleen al completo la tecnología IP.

La iniciativa surge tras la poca trayectoria de negocio en cuanto a datos y aplicaciones de las redes 3G, y la tendencia hacia la convergencia con Internet. Este hecho hace que desde el grupo 3GPP se impulse el concepto de redes 'all-IP'. Con este sistema, los operadores se verían beneficiados por ahorro de costes en la infraestructura y mantenimiento de la red. Además, el grupo se centra en impulsar los servicios de datos en este tipo de redes desarrollando el concepto IMS para el núcleo de red existente IP.

IMS aporta control de sesión siguiendo la arquitectura de Internet adaptada a las redes móviles. Así se dispone de servicios multimedia sobre conmutación de paquetes, para aumentar los ingresos de cada abonado por parte de los operadores. Con IMS es muy sencillo potenciar los nuevos servicios para los usuarios finales, aprovechando toda la infraestrutura y núcleo de red ("*core*") disponible.

Las principales características que ofrece esta tecnología son los siguientes:

- La comunicación, en tiempo real o diferido, está orientada al concepto de 'sesión' entre usuarios o entre usuario y servicio.

- Las sesiones disponen de un nivel de calidad (QoS) adecuado para la transmisión en tiempo real de audio, imagen, vídeo, texto y otros datos.
- A cada usuario, nodo o servicio, se les identifica mediante una URI *("Universal Resource Identifier"*), quedando atrás el manejo de números de teléfono por el uso de nombres al estilo de servicios en Internet.
- El usuario final puede emplear el servicio de presencia, VoIP, videoconferencia, servicios web entre otros, y todos los basados en los protocolos TCP/IP, de manera análoga a como trabajan las aplicaciones en Internet.
- IMS ofrece una infraestructura y capacidad del servicio con el que los operadores pueden implementar sus propias aplicaciones y servicios.

2.3. Implementación de los servicios

Mediante este tipo de red, se facilita la creación e implementación de servicios multimedia, basándose en los elementos conocidos como 'habilitadores del servicio'. ´Los más conocidos dentro de IMS son el de 'presencia' y 'gestión de grupos':

- Presencia: este habilitador de presencia permite a un conjunto de usuarios estar informados acerca de la disponibilidad y formas de comunicación del resto de usuarios del grupo.
- Gestión de listas de grupo: permite a los usuarios crear y gestionar un grupo de usuarios que comparten servicios en la red. Existen mecanismos genéricos de notificación de cambios de grupo y definición de propiedades del tipo privacidad, bloqueo, control de acceso, etc.

Además, otro tipo de actividades que ofrece la red son:

- Servicios personalizados: el usuario puede acceder a servicios personalizados y estandarizados que presente la red. El servicio que ofrece la arquitectura es centrado en el usuario y con una gran escalabilidad.

2.4. Requerimientos IMS

Según se ha especificado IMS, su función es implementar el plano de control de los servicios IP (sobre redes IP) y la señalización del plano de transporte, pero garantizar la conectividad IP es transparente para IMS.

Como evolución desde las redes 3G, IMS hereda las características:

- Interoperabilidad entre distintos operadores: los usuarios de una red IMS tienen la posibilidad de establecer sesiones con usuarios de la red IMS de un operador distinto. Esto se debe a un diseño que garantiza la interconexión con otros operadores. Los datos que se generan en una sesión viajan a través de las redes IP y en las sesiones inter-operador los flujos de señalización recorren todos los dos sistemas IMS.

- El servicio "*roaming*", permite ofrecer a los abonados del sistema el servicio de la red con otros operadores de la misma tecnología (previo acuerdos comerciales entre operadores)

- IMS permite la interconexión con sistemas de redes anteriores, como por ejemplo con las de conmutación de circuitos con el protocolo SS7 para los servicios de voz, las redes GSM y PSTN. Así los usuarios IMS pueden establecer comunicación con usuarios no IMS.

- Interconexión con Internet: asegura el inter-funcionamiento con otras redes IMS e IP externas, pudiéndose establecer sesión entre los usuarios IMS convencionales y los usuarios de Internet.

- Sistemas de seguridad: IMS incorpora seguridad de acceso para los usuarios mediante una publicación propia de la arquitectura denominada ISIM (similar a la SIM en las redes GSM o la USIM en 3G), que permite establecer o no el registro de un usuario en la red mediante una función de autenticación y de registro.

- Calidad del Servicio (QoS): están definidas interfaces por el 3GPP que permiten a IMS controlar y autorizar recursos del subsistema de transporte de redes 3G.

- Provisionamiento de Servicios: para la provisión de servicios, IMS sigue el modelo establecido en Internet, contando con servidores de aplicación que

pueden modificar sesiones multimedia y facilitan el desarrollo de las aplicaciones web hacia el usuario final. Además IMS dispone de plataformas que interactúan con todos los servicios establecidos en redes 3G.

- Tarificación y facturación: para tarificar los servicios multimedia IP intervienen el sistema de tarificación de la red de acceso y el de IMS. De esta forma es posible tarificar los servicios según su duración, contenido y cantidad de datos, ya que desde IMS se registran datos como los usuarios implicados en la sesión, duración, QoS y los asocia a los registros de la der de acceso que se originan como consecuencia del transporte de datos multimedia y la señalización para estos servicios. Además, se soporta la tarificación *offline* como *online*, es decir, tarificación pospago y prepago.

3. Proceso de estandarización

Para asegurar la aceptación en el mercado de una tecnología como IMS, los servicios que ésta ofrece deben ser funcionales para todas las redes existentes de IMS. Esto es posible si todos los productos IMS tienen una estandarización y se verifica que existe interoperabilidad con todos los elementos de la red.

El estándar IMT-2000 (International Mobile Telecomunications-2000) de la Unión Internacional de Telecomunicaciones, ITU ("*International Telecomunication Union*"), es el que describe y se emplea para las redes de tercera generación (3G) siendo el resultado de la colaboración entre varios organismos de estandarización. Entre estos organismos, destacan el 3GPP ("*Third Generation Paternship Project*"), 3GPP2 ("*Third Generation Paternship Project 2*") y el sector de radiocomunicaciones de la ITU, ITU-R ("*ITU-Radiocomunication sector"*) , aunque este último hace referencia a otras áreas distintas a IMS. Además, el organismo OMA ("*Open Mobile Alliance*") aporta estándares sobre el establecimiento de servicios en IMS.

Tanto el 3GPP como el 3GPP2 han creado sus propios estándares de IMS. Ambos organismos emplean protocolos de Internet desarrollados y estandarizados por el IEFT ("*Internet Engineering Task Force*"), e incluso colaboran con éste para desarrollar nuevas especificaciones que cumplan todos los requerimientos específicos para IMS.

3.1. Internet Engineering Task Force (IETF)

El organismo IEFT está constituido por operadores e instituciones investigadoras que trabajan conjuntamente para desarrollar y estandarizar la arquitectura y protocolos basados en IP de Internet. Actualmente, la mayor parte de las bases y protocolos relacionados con IP estandarizados de Internet los ha llevado a cabo el IETF.

Internamente el organismo se divide en grupos de trabajo formados por un número determinado de voluntarios que trabajan de manera independiente y no representan a sus compañías cuando colaboran para el IETF. Los documentos internos que generan estos grupos de trabajo son los denominados "*Internet Draft*" (borrador de Internet), donde diferenciamos dos tipos, los "*submissions"* individuales y los Ítem de grupo de trabajo. Los "*submissions"* individuales son propuestas técnicas desarrolladas por uno o varios voluntarios que si el grupo de trabajo encargado decide que debe ser considerado como principio de tema a desarrollar, se denominará ítem de grupo de trabajo. Una vez llegado a este nivel, si el grupo de trabajo considera que ese ítem

está lo suficientemente desarrollado y especificado, se publicará como especificación de IETF.
Las especificaciones que publica el IETF se denominan 'peticiones de comentarios', RFC ("*Request For Comments*"), y es en este momento cuando se puede tomar el documento como una especificación estable. Existen tres tipos de RCFs:

- RFC estándar: este grupo a su vez se divide en "Propuestas de estándar", "Borradores de estándar", y "Estándar". Generalmente definen los protocolos y sus respectivas extensiones.
- RFC no estándar: se distinguen también tres tipos dentro de este grupo; los "Experimentales", que especifican protocolos que se emplean eventualmente; "Informacionales", que aportan información sobre procedimientos y requerimientos de Internet sobre un determinado tema; y los "Históricos" que son RFCs consideradas obsoletas.
- RFC BCP ("*Best Current Practise*", mejores práticas actuales): ofrecen una recopilación de prácticas actuales para llevar a cabo una determinada tarea generalmente relacionadas con problemas de protocolos.

Pueden encontrarse todos los "*Internet Drafts*", "*Working Group Item*" y los RFC en la web oficial del organismo IETF.
La forma en que se nombran estos documentos es la siguiente:

"Internet Draft" : draft – <nombre del autor>
"Working Group Item": draft – ietf – <nombre del grupo de trabajo >

Los documentos RCF, constan de título, autor, numeración, categoría y otros campos. Para la búsqueda de RFCs, existe en la web oficial de IETF una aplicación denominada "Editor RFC" con el cual es posible realizar una búsqueda filtrando por título, numeración, autor o palabras clave.

3.2. Third Generation Partnership Project (3GPP)

Creada en 1998, este organismo nace con la colaboración conjunta de otros organismos de estandarización como la Asociación de Industria y Negocio de Radio de

Japón, ARIB ("*Association of Radio Industries and Business*") , la Asociación de Estandares de Comunicaciones China, CCSA ("*China Communications Standars Associations*") , el Instituto de Estandarización de Telecomunicaciones Europeo ETSI ("*European Telecomunications Standards Institute*"), el Comité TL de Estados Unidos, el Comité de Tecnilogías de Telecomunicaciones en Japón TTC ("*Telecomunication Technology Comitee*") y la Asociación de Tecnología de Telecomunicaciones de Korea , TTA ("*Telecomunications Technology Committee"*).

Estos organismos pretenden especificar las características de la arquitectura e interfaces de la telefonía móvil para redes de tercera generación basándose en las redes GSM y UMTS. 3GPP ha sido el organismo que ha desarrollado el estándar para IMS apoyándose en anteriores especificaciones.
Los grupos de trabajo de 3GPP desarrollan dos tipos de documentación, las especificaciones técnicas, TS ("*Technical Specification*") y los informes técnicos, TR ("*Technical Report*").

Estas especificaciones se numeran mediante cinco dígitos, en grupos de dos y tres dígitos separados por un punto. Los dos primeros forman el número de serie, y los tres últimos indican la especificación dentro de esa serie. Además, estas especificaciones se agrupan en diferentes publicaciones conocidas como 'Release'. Los más habituales para áreas de IMS son el Release 5 (primera versión de IMS en el año 2000), el Release 6 (segunda generación de especificaciones IMS) y Release 7. Actualmente, 3GPP trabaja en el desarrollo del Release 11, que se centra especialmente en el estudio de evolución de IMS, servicios de interconexión y centralización, aspectos de la arquitectura de los nodos, llamadas de emergencia sobre GPRS y EPS y sistemas de aviso. Toda la documentación puede consultarse en la página web oficial.

El principal cuerpo de estandarización IMS es 3GPP, y otros organismos, como 3GPP2 y TISPAN, han adoptado las bases IMS de 3GPP a sus especificaciones.

3.3. Third Generation Partnership Project 2 (3GPP2)

El organismo Tercera Generación de ("*Third Generation Partnership Project 2*") está formado al igual que 3GPP por AIRB, CCSA, TIA, TTA y TTC. Fue fundado para crear las especificaciones de la red de Tercera Generación en Asia y América del Norte, basándose en los estándares ANSI/TIA/EIA-41 y el de acceso radio CDMA2000.
Internamente se divide en Grupos de Especificaciones Técnicas, TSG ("*Technical Specification Group*"), y el responsable del proceso de estandarización es el Comité de Dirección, SC ("*Steering Committee*"), que aprueba las especificaciones técnicas TS o los informes de progreso TR.

Las especificaciones que publica 3GPP2 se nombran con la forma "A.Bxxx-yyy-R" donde 'A' representa el grupo de especificación técnica; el campo 'B' puede ser una 'S' que indica si es especificación técnica o 'R', un informe técnico; la secuencia 'xxxx-yyy' hace referencia a la numeración de esa especificación o informe, y 'R' indica la revisión del documento.
Toda la documentación puede ser consultada en la página web oficial del organismo.

3.4. Colaboración entre IETF, 3GPP y 3GPP2

En IMS los protocolos que se utilizan son principalmente los mismos que se emplean en Internet. Para ello, tanto IETF como 3GPP y 3GPP2 han trabajado conjuntamente haciendo coincidir los requerimientos de las especificaciones de 3GPP y 3GPP2 con las de los protocolos que desarrolla IETF, y el resultado es que cualquier servicio creado para Internet es válido en IMS. Se pueden ampliar los términos de esta colaboración en las RFC 3113 y 3131.
Para el área de transporte, el principal desarrollo ha sido a manos de 3GPP. El organismo decidió que el protocolo SIP ("*Session Initiation Protocol*") sería el principal para la tecnología IMS. En IETF se creó un grupo de trabajo específico para este protocolo y 3GPP desarrolla servicios de presencia y mensajería instantánea con extensiones de protocolo SIP.

3.5. Open Mobile Alliance (OMA)

El organismo OMA se crea en el año 2002 y su principal objetivo es el desarrollar y habilitar servicios que garanticen la interoperabilidad en las redes. Entre estos servicios destaca para el área de IMS las especificaciones de PoC ('Push to Talk over Cellular'), que permite la comunicación 'half-dúplex' entre dos usuarios móviles mediante voz y texto a modo de 'walkie-talkie', usando habilitadores de presencia y listas de grupos de contactos.

La estructura de esta organización se basa en una serie de grupos de trabajo que dependen de dos posibles comités, el de Procesos y Operaciones y el de Gestión y Planificación. El primero se encarga de los procesos y soporte técnicos mientras que el segundo se centra en plantear y gestionar las diferentes especificaciones que desarrollan los grupos de trabajo. Los documentos que presenta OMA se conocen como '*Release Packages*' , paquetes de divulgación. Cada uno de estos '*Release Package*' experimenta diferentes estados o fases a lo largo de su publicación. La primera fase indica un estado inicial del '*Release*', y una vez aprobadas unas pruebas de interoperabilidad de la especificación, pasa a la segunda fase. En este estado, el documento debe ser aprobado con respecto a la interoperabilidad con otros servicios existentes, alcanzando así a la tercera fase.

Generalmente, para evitar que existan diferentes versiones para los mismos requerimientos en IMS, OMA presenta sus especificaciones y los grupos 3GPP y 3GPP2 trabajan teniéndolas en cuenta con el fin de que todos sean compatibles entre sí. De esta manera se puede asegurar que todas las propuestas y especificaciones cumplan los requisitos de interoperabilidad entre distintas redes de esta tecnología. Además, las especificaciones de OMA también hacen referencia a documentación de IETF. Existe un grupo de trabajo formado por colaboradores de OMA y de IETF que en conjunto analizan y presentan algunas soluciones.
Se puede consultar la información en la página web oficial del grupo.

3.6. Telecoms and Internet converged Services and Protocols for Advanced Networks (TISPAN)

TISPAN ("*Telecoms & Internet converged Services & Protocols for Advanced Networks*") es un cuerpo de estandarización dentro de la organización ETSI ("*European Telecomunications Standards Institute"*) y su principal cometido es el desarrollo de la evolución de las redes a la arquitectura conocida como redes de próxima generación, NGN ("*Next Generation Networking*"). Además, se centra en la evolución de las redes de conmutación de circuitos a las redes de conmutación de paquetes, manteniendo luna única arquitectura que pueda ser empleada en ambas redes y permita la

Esta arquitectura está basada en la conmutación de paquetes, sobre protocolo IP (redes '*All-IP'*). Para ello, TISPAN emplea como base el sistema IMS de 3GPP, a partir de esta documentación especifica normas para el acceso y los servicios de redes fijas para la tecnología IMS.

4. Protocolos principales de IMS

4.1. Protocolos de señalización

Como hemos comentado con anterioridad, las redes IMS se basan en las redes IP, empleando este protocolo a nivel de red (OSI) y TCP/UDP como transporte. En cuanto al nivel de sesión, nos centraremos en los principales protocolos empleados en esta tecnología. Para la señalización, los protocolos centrales son SIP y SDP.

4.1.1. Protocolo SIP

El protocolo SIP (‘*Session Initiation Protocol*’) fue seleccionado por el grupo 3GPP como protocolo principal para la tecnología IMS para el control de de sesión y del servicio, y fue definido por el grupo IETF en la RFC 3261.
Se trata de un protocolo de control que se centra en el nivel de aplicación y que nos permite establecer, modificar y finalizar sesiones multimedia. La finalidad es la existencia de sesiones que intercambien voz, vídeo, texto, imagen u otros archivos en tiempo real.
Es importante notar que este protocolo define los mecanismos necesarios para el intercambio de datos entre usuarios, pero no especifica las caracteríaticas proprias de una sesión, que seríageneralmente labor del protocolo SDP en el caso de IMS.

Como protocolo, SIP emplea algunas funcionalidades de HTTP o SMPT para la navegación por internet o transmisión de correo electrónico, basándose en un modelo cliente-servidor, aunque no va dirigido como HTTP hacia grandes volúmenes de datos sino a mensajes cortos de señalización. Pretende sustituir a los protocolos ISUP que maneja el centro de las llamadas en la Red Telefónica Básica, o el protocolo INAP del control de servicio en redes inteligentes.

Además, la principal ventaja de SIP radica en que es totalmente independiente del protocolo de transporte que se esté empleando en cada momento y del protocolo descriptor de sesión que contenga, permitiendo así establecer cualquier tipo de sesión y con independencia de tipo de acceso.

Se trata de un protocolo punto a punto y emplea mensajes de texto ASCII ("*ASCII text-based*"). Además, sú fácil implementación y gran capacidad para analizar el contenido del tráfico de señalización son unas de sus ventajas.

4.1.1.1. Entidades SIP

Dentro de SIP podemos distinguir dos tipos de entidades, clientes y servidores

- Servidores Proxy: conocidos como '*Proxy Servers'* son los encargados de recibir las solicitudes de los clientes, hacer las modificaciones necesarias y reencaminarlos hacia otros servidores.

- Servidor de Redireccionamiento: en inglés, '*Redirect Servers'*, aceptan las solicitudes SIP y las traduce a la dirección o direcciones de destino para devolvérselas después al cliente.

- Agentes de Usuario: conocidos como UA ('*User Agent'*) son el punto donde finaliza la señalización y emite y recibe las peticiones SIP. Generalmente son los usuarios finales aunque un nodo también puede ejercer esta función (previa carga de un software en un PC, terminal IP o en una estación móvil UMTS).

- Registrador: es aquella entidad SIP que gestiona los registros de los usuarios en la red y mantiene la localización de los mismos de tal forma que para que esos usuarios reciban mensajes pasarán por su correspondiente registrador que los reencamine correctamente hacia el usuario. El usuario indica con un mensaje REGISTER la dirección IP con la que va a ser localizado.

4.1.1.2. Identidades SIP

En el protocolo SIP se definen una serie de identidades de usuario denominadas SIP URI o Tel URL, especificadas en la RFC 3261

4.1.1.2.1. SIP URI y Tel URL

Según se especifica en la RFC 3261 y 2396 de forma habitual en SIP la identidad de un usuario se conoce con el nombre de SIP URI (*'Universal Rosource Indicator'*). Esta identidad es similar a una dirección de correo electrónico manteniendo el siguiente formato:

<sip:user@domain>

<sip:+34600000000@domain>

En el caso de las Tel URL (*'Universal Rosource Locator'*), tendremos un identificador que emplea el número de teléfono del usuario, respetando la siguiente forma (RFC 2806):

Tel:+34600000000

Además, a cada URI o URL puede acompañerle otro tipo de información que sea necesaria con el formato:

sip:user@domain ; parameter = value

Generalmente en estos parámetros se envía información sobre el protocolo de transporte utilizado, en el caso de IMS, bien TCP o UDP.

4.1.1.2.2. Identidades de los usuarios

Dentro de la red IMS cada usuario tiene asociadas dos identidades con las que se le identificará en todas las operaciones, denominadas Identidad Pública de Usuario e Identidad Privada de Usuario. Ésta denominación es específica para las redes IMS.

La Identidad Pública de Usuario (pueden ser una o varias asociadas a un mismo usuario) enruta las peticiones SIP que se dirigen a este usuario y es registrada en la red IMS durante la fase de registro que se establece como requisito para la utilización de la red.

La Identidad Privada del Usuario es conocida por la red y ésta guarda una asociación entre la Identidad Privada y la Pública (una o varias) de las que disponga el usuario.

Un ejemplo de Identidades sería:

-Identidad Pública de usuario: sip:eva.maria@operador.ims.net

-Identidad Privada de usuario: eva.maria@operador.ims.net

4.1.1.3. Peticiones o métodos SIP

Según se especifica en la RFC 3261 existen una serie de peticiones SIP con las que se pueden clasificar los distintos tipos de mensajes:

4.1.1.3.1. Método INVITE

El método INVITE es aquel que nos permite establecer una sesión entre dos agentes de usuario, UAs . Si comparamos con otros protocolos, se podría equiparar al mensaje IAM del protocolo ISUP o el SET UP en Q.931, ya que la información que aporta hace referencia al tipo de datos que se intercambiarán, el destinatario, y el que genera la llamada.

Durante esta petición, la red encamina el mensaje desde el UA emisor hasta el receptor. La red utiliza la información de registro de los usuarios para saber la ubicación de los mismos.

Cuando se reencamina al UA final la petición, la red genera un mensaje 100 TRYING para indicar que las acciones correspondientes se están llevandop a cabo. Del mismo modo, cuando el UA final recibe la petición INVITE, genera otra 100 TRYING para indicar a la red el procesado de la petición. Es en este momento cuando desde el UA final se envía también la respuesta adecuada al tipo de petición que haya procesado. Con INVITE, se pretende establecer una sesión, a lo que el UA contestaría con un 180 RINGING hacia la red. La red encaminaría esta respuesta hasta el UA origen.

Además de estas respuestas existen muchas otras posibilidades como se indica posteriormente en la tabla genérica (Tabla 1).

4.1.1.3.2. Método BYE

Mediante la indicativa BYE se permite liberar una sesión en curso. Este método puede iniciarlo tanto el UA que generó la petición de sesión como el UA destino. Cuando el UA que decide terminar la sesión envía la petición BYE a la red, ésta la reencamina al

UA destino, y se contesta con el mensaje 200 OK si se termina la sesión de forma correcta.

4.1.1.3.3. Método Register

Con el método REGISTER, un UA indica al ‘Registrar’ su petición de registro en la red, el cual procesa dicha petición y genera una determinada respuesta. Normalmente contesta con ‘401 UNAUTHORIZED’ a la primera petición de registro ya que los datos del usuario no están autenticados en ese momento. En la cabecera del mensaje, se envían datos para la autenticación del usuario (método ‘desafío’ que veremos más adelante) El UA volvería a lanzar la petición de registro pero esta vez incluyendo en la cabecera datos que responden al desafío propuesto por la red. Si el ‘Registrar’ lo valida, contestaría con 200 OK.

4.1.1.3.4. Método CANCEL

Utilizado para terminar una llamada que esté en curso pero no una que ya esté establecida, ya que en este caso finalizaría con el método BYE. Cuando un UA envía un CANCEL, la red contesta 200OK si se procesa esta petición, igual que el UA destino al recibirlo.

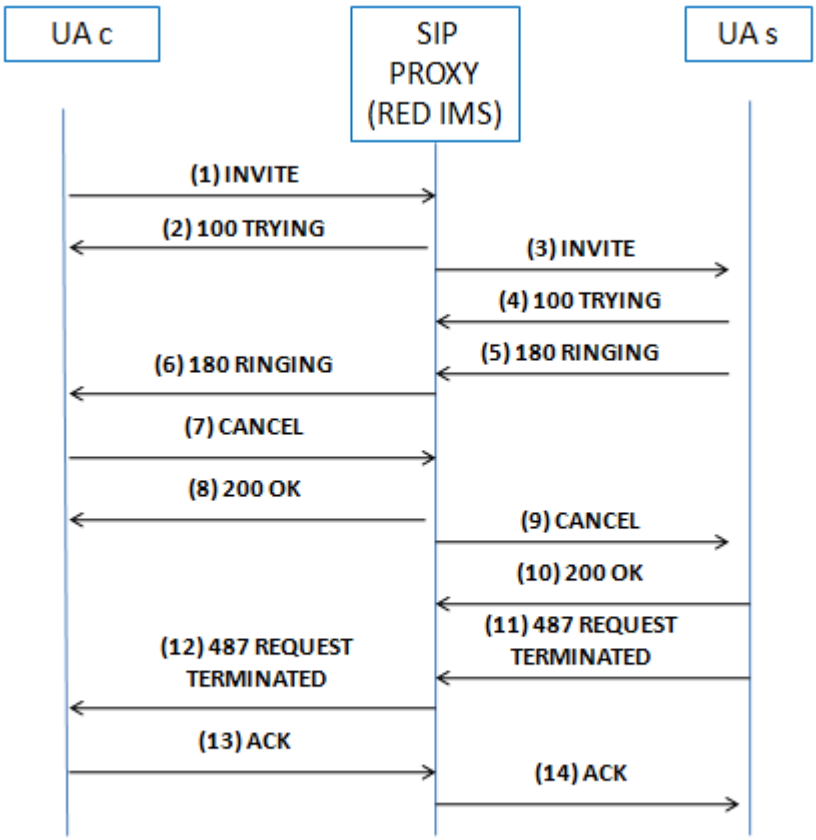


Figura 2. Ejemplo de flujo de mensajes SIP

4.1.1.3.5. Método ACK

Mediante este método es posible indicar que el proceso petición-respuesta se ha resuelto de manera satisfactoria. Este mensaje se genera para confirmar, ya sea a la red o al UA final, que la respuesta a la petición se ha procesado correctamente.

4.1.1.4. Respuestas SIP

Una vez se reciben y procesan las peticiones SIP, el UA destino o servidor en su caso devuelven una respuesta SIP numerada según su naturaleza de la siguiente forma:

Tabla 1 Tipo de respuestas en SIP

Clase	Interpretación	Comentario
1xx	Información	El requerimiento se ha recibido pero la petición está en curso
2xx	Éxito	Requerimiento recibido, entendido y aceptado
3xx	Reencaminamiento	La petición requiere más procesos para determinar si se realizará o no
4xx	Error cliente	El requerimiento no es soportado por el UA destino o servidor
5xx	Error servidor	El servidor no es capaz de resolver una petición que parece correcta
6xx	Error global	El requerimiento no lo puede procesar ningún servidor

El nombre de la respuesta SIP está formado por el número correspondiente según la tipología que proceda y una componente textual descriptiva como ya hemos visto anteriormente. Un ejemplo es '100 TRYRING'

4.1.1.5. Formato del mensaje

El formato del mensaje SIP se compone de tres bloques, línea de inicio, cabecera y cuerpo del mensaje. La línea de inicio y las cabeceras tratan de definir el mensaje mientras que el cuerpo lleva los datos de señalización a intercambiar entre ambos extremos. Generalmente, en IMS, se utiliza el formato del protocolo SDP para la descripción de la sesión en el cuerpo del mensaje SIP.

4.1.1.5.1. Línea de inicio

La línea de inicio, dependiendo si se trata de un mensaje de petición o de respuesta se conoce como *'request-line'* o *'status –line'*

La línea de petición ('request-line') está formada por el nombre del método, la 'request-URI', que indica el destinatario, y la versión del protocolo que se está empleando. Para la versión del protocolo hasta ahora siempre se señala SIP/2.0
La línea de estado ('status-line'), que aparece con los mensajes de respuesta SIP, presenta un formato que comienza con la versión del protocolo (SIP/2.0) y la respuesta

SIP. Recordamos que la respuesta SIP está formada por el indicador numérico según la clase y el texto.

Ejemplos de estas líneas serían:
INVITE sip:eva@ims.operador.es SIP/2.0, como línea de petición.
SIP/2.0 200 OK, como línea de estado.

4.1.1.5.2. Cabecera

Según se define en la RFC 2822, el formato que presenta la cabecera del protocolo es:
<headre_name>:<header_value>
Donde <header_name> indica el nombre de la cabecera seguido del valor de la misma, <header_value>. Es posible que existan varias cabeceras con el mismo <header_name> dentro de un mismo mensaje SIP, cambiando el campo valor. Los campos más significativos dentro de la cabecera se describen a continuación:

- Via: en este campo se indican los servidores 'proxy' por los que salta una petición SIP. Esta información es necesaria para el retorno del mensaje respuesta a dicha petición. Presenta el siguiente formato:
  Via:SIP/2.0/<transport><address>:<port>;branch=<ID>

  Donde:
  - <transport> indica el protocol se transporte utilizado.
  - <address> indica la dirección IP que envía en mensaje.
  - <port> hace referencia al puerto enpleado en el envío.
  - <branh> identifica la transación. Siempre comienza por los caracteres 'z9hG4bK'

- To: mediante este campo de la cabecera conocemos la dirección SIP URI o TEL URL del receptor. Esta información se utiliza en la fase de registro y en otras aplicaciones pero no como parámetro de enrutamiento. Puede presentar una cadena de caracteres ("Name") previa a la dirección URI como información adicional. También puede aparecer una etiqueta ("Tag") como método de identificación de mensaje. Por tanto, presenta la forma:
  To: "Name" <URI>; tag=<tag_value>

Un ejemplo podría ser: To: “Eva” sip:eva@ims.operador.net

- From: al igual que ‘To’, mediante ‘From’ se identifica la SIP URI o TEL URL del emisor, manteniendo el mismo formato, con la diferencia que en este caso el parámetro ‘tag’ es opcional.

- Call-ID:

Este campo contiene una identificación única de la sesión. El formato es el siguiente:
Call-ID: <identifier>@<domain>
Donde:

  - <identifier> es un número hexadecimal
  - <domain> se representa con la dirección IP del servidor de dominio que lo genera

- Cseq: campo que permite conocer la petición a la que va vinculada una respuesta SIP. Contiene el número de la secuancia y el nombre del método, con el siguiente formato:
  Cseq: <seq_number><method>

- Max-Forwards: indica el número máximo de saltos permitido para el mensaje SIP. Su valor de inicio es el valor máximo asignado y decrementa su valor pòr cada salto.

- Contact: alamacena las URIs en las cuales es posible localizar al UA. El formato ue presenta es:
  Contact: “Name” <URI>=<optional_parameter>, donde el parámetro opcional presenta información adicional, generalmente relacionado con la validez temporal de la petición.

- Record-Route: almacena la dirección del proxy SIP que inserta la cabecera mientras se hace el enrutamiento de la petición. De esta forma queda registrado por dónde tienen que pasar las siguientes peticiones que se creen dentro del mismo diálogo.

Además de estos parámetros de cabecera, cuando los mensajes SIP contienen descriptores de sesión en el cuerpo del mensaje, se utilizan las cabeceras:

- Content-type: indica el tipo de descrptor del cuerpo del mensaje. En IMS, generalmente se utiliza el protocolo SDP, indicándose del modo 'application/sdp'

- Content-Lenght: indica el número de octetos del cuerpo del mensaje.

4.1.1.5.3. Cuerpo del mensaje

El cuerpo del mensaje contiene la información que se intercambian los dos extremos en la comunicación. Gracias a la información de la línea de inicio y la cabecera es posible la comunicación extremo a extremo. Además, en la cabecera es donde se indica el tipo de mensaje que se está enviando, y su formato. En IMS, el más utilizado es SDP, que ya veremos más adelante. La información relativa al tipo de formato y la longitud del cuerpo del mensaje (en octetos) se indica en la cabecera mediante los campos 'Content-Type' y 'Content-Lenght' que hemos mencionado en el anterior apartado.

Como está definido en la RFC 2045 emplea el formato descrito por MIME, el cual permite que el cuerpo del mensaje conste de varias partes cada una con un formato distinto, lo cual vendría especificado en la cabecera de la siguiente forma:

Content-Type: multipart/mixed; boundary = 'delimiter'

Donde 'boundary' es un parámetro que indica la frontera entre las partes del mensaje.

4.1.2. SDP

El protocolo de texto SDP ('*Session Description Protocol*') fue definido por el grupo de estandarización IETF y está definido en la RFC 2327. Se trata de un protocolo destinado a la descripción de los parámetros que son necesarios para la notificación, el inicio y establecimiento de una sesión multimedia. Al igual que SIP, es transparente el protocolo de transporte que se esté utilizando en cada instante.

La descripción de la sesión que realiza SDP consiste en una serie de líneas de texto con la forma <type>=<value., donde el campo denominado 'tipo' (<type>) es un único

carácter y 'valor' (<value>) puede estar formado por dos parámetros, que en este caso se separarían por un espacio en blanco. Sin embargo, no se permite el espacio en blanco entre los parámetros 'type' y 'value' y el carácter '='.

De modo genérico, para describir una sesión SDP emplea en orden estricto una serie de datos:

- Descriptores de nivel de sesión: este tipo de descriptor es obligatorio, y muestra detalles relacionados con todo el conjunto de la sesión y los flujos de datos.
- Descriptores de tiempo: indican el comienzo y finalización para la sesión.
- Descriptores de media: son opcionales, y se centran en detalles que aplican sobre el flujo de datos de media.

Además, es importante notar que pueden existir varios descriptores de media dentro de una misma sesión.

4.1.2.1. Campos del Mensaje SDP

El mensaje SDP, consiste en una serie de descriptores de sesión(comienzan con el campo 'v=') seguidos de o no de descriptores de media (campo 'm='). Los campos del mensaje SDP deben colocarse en estricto orden como se especifica en la siguiente tabla:

Tabla 2 Campos de la cabecera en mensaje SDP

CAMPOS SDP **Session level description**
v= (protocol version)
o= (owner/creator and session identifier)
s= (session name)
i= (session information)
u= (URI of description)
e= (email address)
p= (phone number)

c= (connection information)
b= (zero or more bandwidth information lines)
Time level description / Time descriptions (“t=” and “r=” lines)
t= (time the session is active)
r= (zero or more repeat times)
z= (time zone adjustments)
k= (encryption key)
a= (zero or more session attribute lines)
Media level description if present, one or more Media descriptions
m= (media name and transport address)
i= (media title)
c= (connection information)
b= (zero or more bandwidth information lines)
k= (encryption key)
a= (zero or more media attribute lines)

A continuación analizaremos los campos más representativos de SDP

- Versión de protocolo: identificado como ‘v=’ aporta como su nombre indica el número de versión del protocolo que se utiliza. En la actualidad toma siempre el valor 0.

- Origen: identificado como ‘o=’ indica quién originó la sesión, informando sobre el nombre de usuario y la dirección del host del usuario, el identificador de la sesión y el número de versión de la sesión. Generalmente con este campo se identifica globalmente la descripción de la sesión, tomando el siguiente formato:

  o=<username> <sess-id> <see-version> <nettype> <addrtype> <unicast-address>

  Donde cada uno de los campos que lo forman indicant:

  - <username> es el nombre de usuario en el host origen o se sustituye por ‘-‘ si el host origen no permite el concepto. Si un host que no permite este campo lo recibe dentro del mensaje, ignora el valor ‘username’.

- <sess-id> identifica a la sesión junto con otros parámetros y es una cadena numérica. Representa un máximo de 64 bits, por lo que el valor será menor que 2^{24}-1.
- <sess-version> es el número de versión para esta descripción de sesión en particular y se emplea para la petición y respuesta del manejo de sesiones. Inicialmente tendría un valor menor que 2^{63}-1 que es decrementado cada vaz que se realiza alguna modificación en los datos de la sesión.
- <nettype> es una cadena de caracteres que proporciona información sobre el tipo de red. La cadena 'IN', por ejemplo, hace referencia a internet
- <addrtype> está representado por una cadena de caracteres que indica el tipo de dirección IP utilizado, teniendo como posibilidades 'IP4' o 'IP6'.
- <unicast-address> , representa la dirección global de la máquina que ha iniciado la sesión.

- Nombre de Sesión: identificado con 's=' es un valor que se trata como una cadena de caracteres y sólo puede existir un campo 's' por sesión.

  s=<session name>, 'session name' es el nombre identificativo y contiene caracteres ISO 10646

- Datos de conexión: se representa con 'c=' y contiene los datos de conexión de la sesión, donde hay que enviar el tráfico una vez establecida la sesión. Sigue el formato:

  c=<nettype><addrtype><connection-address>

  En cada descripción de media, es imprescindible este campo. SI se da el caso en el que existan varias descripciones de media distintas, debe haber un campo 'c=' por cada una de ellas. Como ya hemos visto anteriormente la indicación de cada campo que forma 'c' un ejemplo de contenido sería:

  c=IN IP4 <unicast_IP_address>

- Ancho de banda: representado con el caracter 'b=' es un campo opcional que indica el ancho de banda que puede usarse para dicha sesión. El formato que sigue es el siguiente:

  b=<bwtype>:<bandwidth>

  Es un parámetro que se recibe como dato de nivel de sesión y de media.

- <bwtype> es un parámetro alphanumérico que toma usualmente los valores:

  -RR, indicando que el ancho de banda empleado para algunos usuarios es el permitido para RTCP durante la sesión RTP.

  -RS, que indica el ancho de banda en RTCP para los datos de los emisores activos.

- <bandwith>, se interpreta como los bits por segundo de RR o RS.

- Campos de tiempo: se especifican con 't=' e indican el comienzo y final de la sesión. Pueden existir varios campos 't=' donde cada 't' adicional indica unidades de tiempo adicionales que la sesión permanece activa.

  Se indica con el formato t=<star-time> <stop-time>, donde:

  <start-time> es un parámetro numérico que indica cuando la sesión toma comienzo. SI toma el valor '0' se espera que la sesión comience en ese mismo momento.

  <stop-time> indica el tiempo en el que acaba la sesión. Si su valor es '0' la sesión no tiene que finalizar por defecto.

A continuación de los parámetros temporales, aparecen los campos de extensión SDP. Se pueden agrupar en descriptores de nivel de sesión, de media, o de ambos al mismo tiempo. En la siguiente figura se muestran dichas variables. Este tipo de campo se identifica con el símbolo 'a=' derivado de la palabra atributo. Puede tener dos tipos de formato:

a=<attribute> , donde la presencia de este tipo de atributo indica que es descriptor de media.

a=<attribute>:<value>, donde un determinado valor acompaña al campo atributo.

Tabla 3 Descriptores de nivel de sesión y de media de extensión para SDP

Tipo	Nivel (S= Sesión, M= Media)
Category (a=cat)	S
Keywords (a=keywds)	S
Name and version of tool (a=tool)	S
Packet time (a=ptime)	M
Maximum packet time	M

Tipo	Nivel (S= Sesión, M= Media)
(a=maxptime)	
Receive-only mode (a=recvonly)	SM
Send and receive mode (a=sendrecv)	SM
Send-only mode (a=sendonly)	SM
Inactive (a=inactive)	SM
Whiteboard orientation (a=orient)	M
Conference type (a=type)	S
Character set (a=charset)	S
Language tag (a=sdplang)	SM
Quality (a=quality)	M
Format specific parameters (a=fmtp)	M
Rtpmap (a=rtpmap)	M
Frame rate (a=framerate)	M

- Campo de descripción de media:

Una sesión debe contener una serie de descriptores de media, los cuales se identifican con 'm='. Generalmente, sigue el formato:

'm=<media> <port> <proto> <fmt>… donde cada uno de los parámetros indica:

- <media>: indicativo del tipo de dato, ya sea audio, video u otro tipo de archivo.
- <port>: indica el puerto de transporte donde los datos serán enviados. Los valores que puede tomar son de 0 a 65535 salvo para el protocolo UDP, que debe ser 0 ó valor comprendido entre 1024 y 65535.
- <proto>: este es el parámetro que indica el protocolo empleado para el transporte
- <fmt>: es un descriptor del contenido del mensaje. Para datos de audio, se define en la carga del mensaje del protocolo RTP. Es indicativo de si la carga es con formato estático o dinámico. Indica el tipo de códec que soporta el terminal emisor. Para que sea posible establecer la sesión, tanto el emisor como el

receptor han de soportar al menos un códec en común para cada tipo de flujo de media que se intercambia.

Un ejemplo de mensaje SDP es el siguiente:

```
v=0
o=- 2790844476 2865552807 IN IP4 172.198.66.10
s= sessionname
c=IN IP4 172.17.66.10
t=0 0
m=audio 20000 RTP/AVP 97 98 99 100 102 108
b=RS:800
b=RR:2400
a=rtpmap:97 AMR/8000
a=fmtp:97 mode-set=0,2,4,7; mode-change-period=2; \
mode-change-capability=2; mode-change-neighbor=1
a=rtpmap:98 AMR/8000/1
a=fmtp:98 mode-set=0,2,4; octect-align=0; mode-change-period=2; \
mode-change-capability=2; mode-change-neighbor=1
a=rtpmap:99 AMR/8000/1
a=fmtp:99 mode-set=0,2,4; octect-align=1; mode-change-period=2; \
```

Figura 2.Formato de mensaje SDP

Si analizamos el mensaje observamos que la versión es ‘0’, y el origen de la sesión (identificada con los números que aparecen en el campo ‘o’) viene de un usuario con dirección 172.198.66.10 en tipo de red Internet (‘IN’) con protocolo Ipv4 (‘IP4’).
El tiempo de comienzo y final se indica con ‘0’, por lo tanto el envío de paquetes puede realizarse inmediato una vez establecida la sesión y no tiene tiempo estimado de finalización por defecto. Con los descriptores de media, sabemos que es una sesión destinada al intercambio de datos de audio, el protocolo de transporte será RTP/AVP, es decir,RTP/ UDP (según se define en la IETF) y a continuación los códecs soportados.
Para una descripción detallada de las posibilidades de contenido de un mensaje SDP, podemos consultar la RFC 2327.

4.2. Otros protocolos

Además de SIP y SDP, dentro de la red IMS cabe destacar el protocolo de nivel de sesión RTP para el transporte de datos en tiempo real, como voz o vídeo sobre UDP que a la vez trabaja sobre IP a nivel de red. Mediante estos protocolos no se puede asegurar el transporte extremo a extremo seguro, en cuanto al orden de llegada de los

paquetes. Por tanto, surge la necesidad de introducir un mecanismo de control para el flujo de datos en tiempo real de voz o vídeo.
El protocolo RTP ha sido diseñado para funcionar con su protocolo auxiliar RTCP para mantener la calidad durante la transmisión.

4.2.1. RTP

Definido por la RFC 3550 del grupo IETF, el protocolo RTP ('Real Transport Protocol') permite identificar la tipología de datos que se está transportando así como la inclusión de nuevos marcadores o etiquetas temporales para poder identificar el instante de tiempo en el que se emite el mensaje e incluir los números de secuencia para la detección de pérdida de paquetes. Se implementa generalmente sobre UDP/IP, pero es importante notar, que RTP no garantiza la entrega del paquete en el destino.
RTP es un protocolo tanto 'unicast' como 'multicast', pudiendo encamirnar conversaciones a distintos destinos.

4.2.1.1. Formato del mensaje

El protocolo RTP transporta los mensajes sobre paquetes que constan de cabecera de longitud fija , con 12 octetos, y cuerpo del mensaje o carga útil de longitud variable.

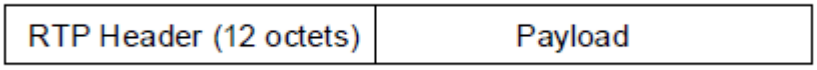


Figura 3 Formato del mansaje RTP

Los campos que forman la cabera son los siguientes:

- V (2 bits): indica el número de versión de protocolo que se utiliza. Actualmente es la número dos.
- P (2 bits): si su valor es '1', indica que la carga tiene datos de relleno. La carga útil debe tener una longitud en octetos múltiplo de cuatro. En el ùltimo octeto de la carga, se indica el número de octetos a ignorar.
- X (1 bit): si su valor es '1', indica que hay extensión de cabecera.
- CC (4 bits): indica el número de indentidades CSRC ligadas a la cabecera.

- M (1 bit): bit de señalización para la capa de transporte.
- PT (7 bits): identifica el contenido de contenido qu lleva el paquete, indicando el tipo de codificación.
- Sequence number (16 bits): campo mediante el cual es posible detectar la pèrdida de paquetes. Representa un contador que toma un valor inicial aleatorio, y se incrementa en una unidad cada vez que se envía un paquete.
- Time Stamp (32 bits): se trata de marcas temporales para controlar el retardo y la fluctuación del sistema.
- Synchronization source (32 bits): campo que permite identificar la fuente que emite el mensaje. AL comienzo d e cada sesión, el emisor escoge su número de SSRC.
- Contributing source (16 bits): permite la posibilidad de incluir hasta 16 bits para este campo. El número de bits se indica en el campo CC.

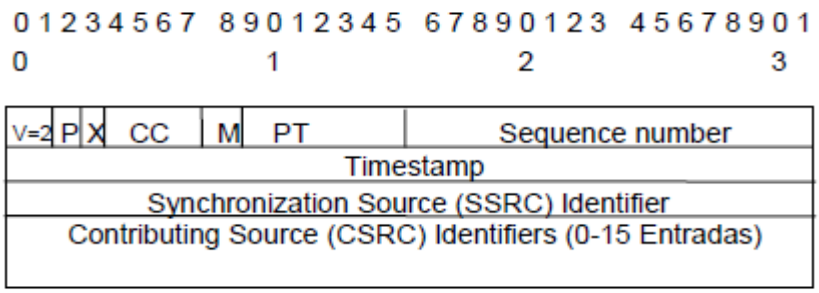


Figura 4. Formato de cabecera RTP

4.2.2. RTCP

El protocolo RTCP ("*Real Time Control Protocol*") funciona como control de flujos RTP transmitiendo mensajes de control periódicos a todos los participantes de la sesión. Actúa siempre en conjunto con RTP.

El control se realiza mediante cinco tipos de paquetes:

- SR ("*Sender Report*"): contiene estadísticas para la transmisión y la recepción de paquetes de los participantes de la sesión que son emisores y además son activos.

- RR ("*Receiver Report*") contiene estadísticas de recepción para los participantes que no son emisores pero sí son receptores dentro de una sesión.

- SDES ("Source *Description*"): aporta datos de descripción de la fuente tales como el nombre,la dirección de correo electrónico, el teléfono, etc.

- BYE: permite indicar el fin de su participación en una sesión a un determinado usuario o estación.

- APP: es un paquete de señalización específico para una aplicación. Los datos que transporta dependen por tanto de la aplicación que se requiera.

El control de flujo de RTP que se lleva a cabo mediante RTCP se realiza mediante una evaluación del número de participantes de una sesión (fuentes y receptores) sobre el que se calcula un intervalo de tiempo para el envío de SR o RR según proceda. De esta forma la cantidad de datos transmitidos para el control es reducida en comparación con el volumen global de datos que se maneja en la sesión. Cuanto más elevado es el número de participantes en la sesión, menos precisa es la visión que tiene cadaparticipante del estado de la red.Los paquetes que se transmiten con más frecuencia son SR y RR.

Otra función de importancia de RTCP es la identificación de los distintos emisores de la red. Se utiliza para ello los paquetes SDES, que incluyen el campo CNAME ("*Canonical Name*"). Este campo es un identificador único y permanente del nivel de transporte para cada emisor.

5. Arquitectura de IMS

5.1. Planos en IMS

En la estructura de las redes de nueva generación, pueden diferenciarse cuatro capas totalmente diferenciadas con distintas funcionalidades, como se observa en la figura 5. A estas capas también se les denomina 'planos' del IMS.

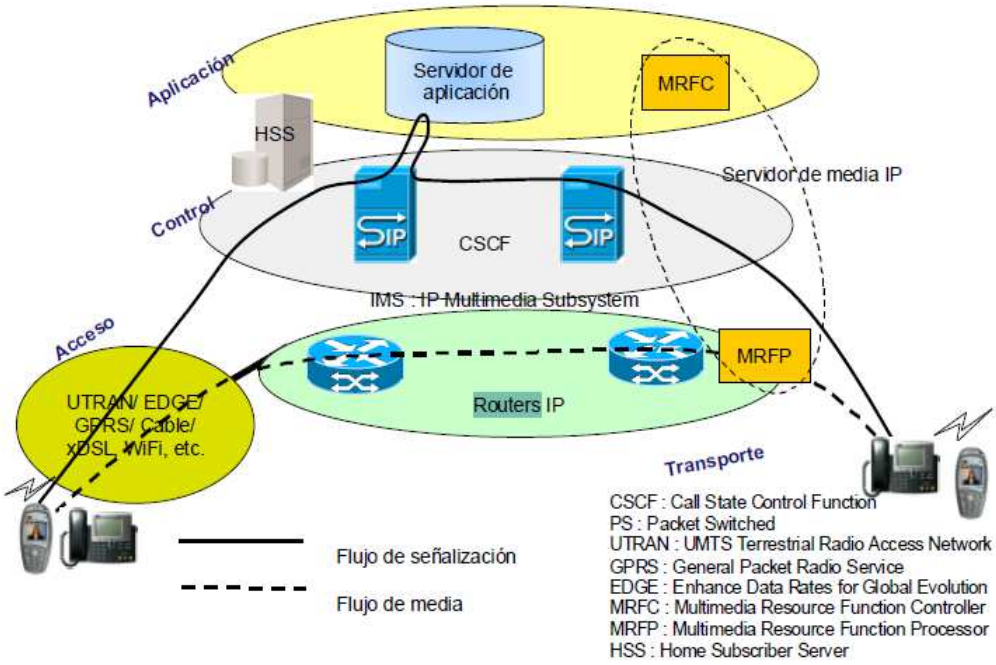


Figura 5. Arquitectura genérica para IMS

- Capa de acceso: representa cualquier tipo de acceso con alta velocidad, como por ejemplo UTRAN, CDMA2000, redes de banda ancha, de cable, WI-FI…Pero las redes de acceso tendrán que disponer de capacidad para la conmutación de paquetes, ya que la señalización de IMS se basa en este mecanismo. En el caso de tratarse de una red de conmutación de circuitos habrá que disponer de conversión de la señalización de circuitos a la señalización de conmutación de paquetes.

- Capa de transporte: hace referencia a una red IP. El transporte se realiza mediante *routers (edge routers* para el acceso y *core routers* para el tránsito

de datos) que se encurntran conectados mediante una red de transmisión. Para IMS es transparente la pila protocolaria que haya por debajo del nivel IP.

- Capa de control: es la capa donde se centra IMS, tomando el control de toda la señalización e interacción con la capa de aplicación donde se encuentran los diferentes servicios (CSCF). Aquí, los nodos IMS llevan el control de las sesiones de los usuarios. Toda la señalización dentro de IMS funciona sobre TCP/IP ó UDP/IP.

- Capa de aplicación: está formada por los servidores de aplicación y servidores de media que proporcionan los servicios a los usuarios. Este es el principal beneficio para los operadores, que pueden integrar nuevos servicios y funcionalidades sobre la capa de control.

A continuación, conoceremos los principales nodos que forman la arquitectura IMS.

5.2. Principales nodos en IMS

Los nodos que forman la red IMS son las entidades lógicas que tienen definidas las funciones desarrolladas por el grupo de estandarización 3GPP. Para diseños de red de implementación real, las funciones estandarizadas pueden distribuirse de distinta forma, e integrar en un mismo nodo varias funcionalidades. Cada nodo de la red IMS tiene su correspondiente IP, por lo que para centrarnos en el nivel de sesión, consideraremos que está garantizada la conectividad IP entre los nodos que forman la red. En la siguiente figuran se aprecia la arquitectura del estándar 3GPP.

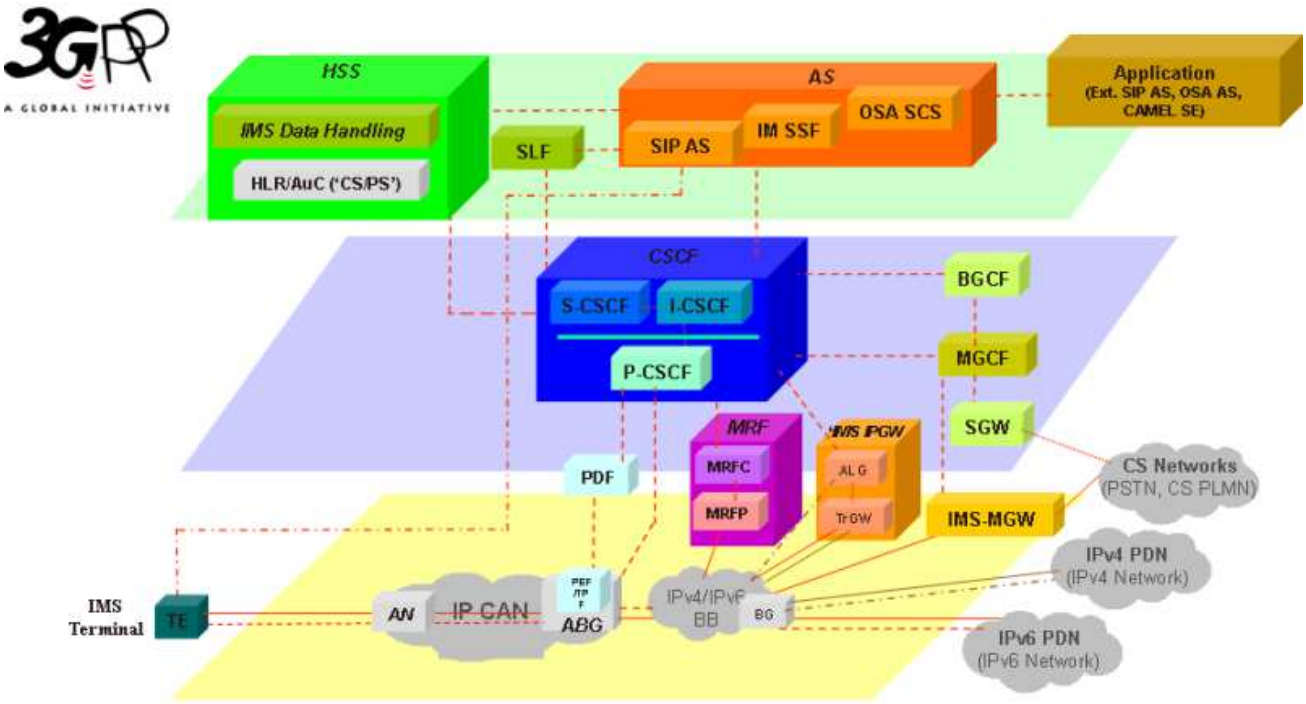


Figura 6. Arquitectura de red 3GPP

5.2.1. CSCF

La función CSCF (Call Session Control Function o Función de Control de Sesión de Llamada) es la principal dentro de la red IMS. Está definida tanto por 3GPP como por 3GPP2 y utiliza el protocolo SIP (IETF SIP RFC 3261) para establecer, modificar y terminar una sesión multimedia.

Es por tanto un servidor SIP, que procesa la señalización de dicho protocolo dentro de la red IMS, y desempeña las siguientes funciones:

- Función de control de sesión de llamada *Proxy*, P-CSCF ("*Proxy Call Session Control Function*")
- Función de control de sesión de llamada i, I-CSCF ("*Interrogatong Call Session Control Function*")
- Función de control de sesión de servidor , S-CSCF ("*Serving Call Session Control Function*")
- Servicio de Emergencia, E-CSCF ("*Emergency CSCF*")
- Función de Control de Pasarela de Salida, BGCF ("*Break-out Gateway Control Function*")
- Función de Control de Entradas, BCF ("*Break-in Control Function*").

Estas entidades lógicas se encargan de cursar tráfico tanto de manera conjunta como de modo independiente, según la configuración de la red.
El grupo 3GPP describe en su especificación técnica TS23.228 los nodos P-CSCF, I-CSCF, S-CFCS, E-CSCF y el BGC. A continuación, resumimos las características de estas funcionalidades del nodo CSCF.

5.2.1.1. Proxy CSCF (P-CSCF)

El nodo P-CSCF, descrito en la especificación TS 24.229 3GPP, es el primer punto de contacto con la red IMS, y actúa como entrada y salida de la misma, por lo que todas las peticiones iniciadas desde un terminal IMS se reciben en este nodo. El UE, encuentra la dirección del P-SCFS mediante un mecanismo de búsqueda específico para este tipo de terminales.
Las funciones principales de este nodo son:

- Enviar la peticiones de registro SIP (SIP REGISTER REQUEST) que recibe desde un UE hacia la red (hacia el I-CSCF). Además, también reenvía los mensajes SIP desde un UE hacia el S-CFCF y desde el S-CFCF hacia el UE.

- Verifica que todas las peticiones SIP que recibe del terminal IMS son acordes a la normativa que deben cumplir.

- Comprime y descomprime los mensajes SIP (soporta las especificaciones descritas en el SIP RFC 3261) ya que incluye un compresor/descompresor de mensajes SIP. Los terminales IMS también disponen de esta función.

- Almacena la información de registro de los UE. Además, asegura la identidad del usuario al resto de nodos de la red, y durante la sesión queda registrada dicha identidad. El P-CSCF recibirá un mensaje de registro (REGISTER) desde el UE y lo encaminará hacia el I-CSCF. Por tanto, este nodo retiene la información de registro y de sesión.

Puede haber varios P-CSCF en una misma red, y cada uno abastece a un número determinado de terminales, dependiendo de su capacidad.

5.2.1.2. Interrogating CSCF (I-CSCF)

El I-CSCF es el punto de contacto entre la red IMS del operador, para la señalización de un usuario de esa red. I-CSCF está definido en la especificación técnica 3GPP TS 24.229 y soporta especificaciones SIP definidas en el RFC 3261.

La principal función del I-CSCF es asignar a cada usuario un S-CSCF en la fase de registro. La petición de registro llega al I-CSCF desde el P-CSCF o desde otra red, y el I-CSCF actuaría en este caso como primer punto de contacto. Además, tiene un interfaz de comunicación con el HSS (Home Subscriber Server), utilizando el protocolo DIAMETER (RFC 3588).

La dirección del S-CSCF que se asigna a cada usuario, la toma del HSS (para un usuario ya registrado). Una vez que conoce la dirección de S-CSCF de un usuario, encamina la petición de registro hacia dicho S-CSCF (mensaje SIP, REGISTER) . Además, también dirige los mensajes SIP que provienen de otra red hacia el S-CSCF o hacia los AS.

En las redes de los operadores, es posible que haya varios de estos nodos funcionando de manera concurrente. Puede generar Registros de Datos de Llamada, CDR ("*Call Data Records*"), empleados para la tarificación.

5.2.1.3. Serving CSCF (S-CSCF)

S-CSCF es un servidor SIP que se especifica en TS 24.229 de 3GPP, y realiza el control y mantenimiento de la sesión del UE. Es la función principal de la señalización para las redes IMS. Actúa como gestor de las peticiones de registro SIP y guarda la información necesaria durante la fase de registro (la información la proporciona el HSS). Al igual que el I-CSCF, el S-CSCF emplea el protocolo DIAMETER en el interfaz de comunicación con el HSS.

Los datos que toma del HSS son los relativos al perfil del usuario, donde también se encuentra toda la información de perfil del servicio. Para la correcta autenticación del usuario en la red, el HSS proporciona los vectores de autenticación del usuario.

Además, el S-CSCF le indica al HSS que es el servidor asignado a un usuario durante la fase de registro

Las principales funciones de control que desempeña este nodo son:

- Controla la sesión en los terminales registrados y rechaza toda comunicación con Identidades Públicas de Usuario que no estén permitidas (‘barred’)
- Posibilidad de actuar como Proxy SIP (RFC 3261) aceptando y atendiendo peticiones internamente o reenviándolas donde proceda.
- Posibilidad de actuar como UA SIP generando sesiones SIP y finalizándolas cuando sea necesario.
- Interacciona con los AS.
- Maneja los estados de registro y de sesión.

El encaminamiento SIP, se realiza de acuerdo a los procedimientos de 3GPP y 3GPP2. Para el tráfico entrante, el S-CSCF envía las sesiones al P-CSCF, cuya dirección almacenó en la fase de registro. Para el tráfico SIP de salida, el S-CSCF obtiene la ruta a través del DNS / ENUM. Además, como ya hemos comentado, S-CSCF interactúa con el HSS para obtener los datos de subscripción e intercambiar información de autenticación usando DIAMETER. Con la información recibida del HSS, el S-CSCF es capaz de interpretar si el AS puede recibir la información de petición de establecimiento de sesión SIP (entrante a la red) para asegurar un apropiado mantenimiento de la sesión.

En cada red IMS generalmente hay varios nodos que implementan esta función, y siempre debe haber al menos uno en cada una de ellas.

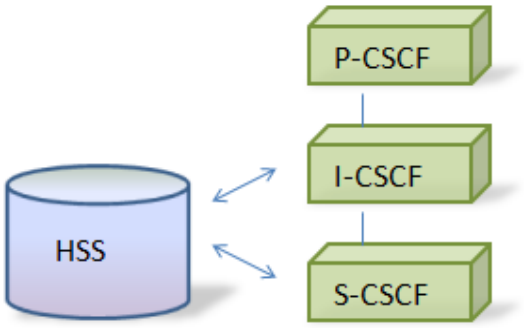


Figura 7.Funciones del CSCF que interactúan con HSS

5.2.1.4. Combined CSCF (Combined ISP)

El nodo ISP, combina las funciones de I-CSCF, S-CSCF y P-CSCF, y la señalización SIP entre estas tres funciones se sustituye por una comunicación interna dentro del propio equipo. La función P-CSCF utiliza el parámetro 'Nombre de Dominio' para conocer mediante un algoritmo de búsqueda si el I-CSCF se encuentra en el mismo equipo o no. Del mismo modo, el I-CSCF realiza una búsqueda similar para encontrar el S-CSCF en el mismo equipo.

5.2.1.5. BGCF

La función principal de este nodo es seleccionar la pasarela de salida para encaminar peticiones SIP cuando no es posible realizarlo mediante el procedimiento habitual en IMS (SIP-URI). EL S-CSCF es el que envía al BGCF la información relativa a si es posible encaminar la petición SIP mediante SIP-URI porque su destino es la red IMS, o de lo contrario, si la petición va dirigida a la red fija PSTN.

Cuando va dirigido a la PSTN es el momento en el que entra en juego el BGCF para enrutar adecuadamente la petición. Por lo general, el BGCF emplea al MGCF (Media Gateway Control Function) de la propia red IMS para que interactúe con la red de conmutación de circuitos. PSTN. Si para llegar al PSTN hay que enviarlo a otra red IMS, el BGCF envía la petición SIP al BGCF de la otra red.

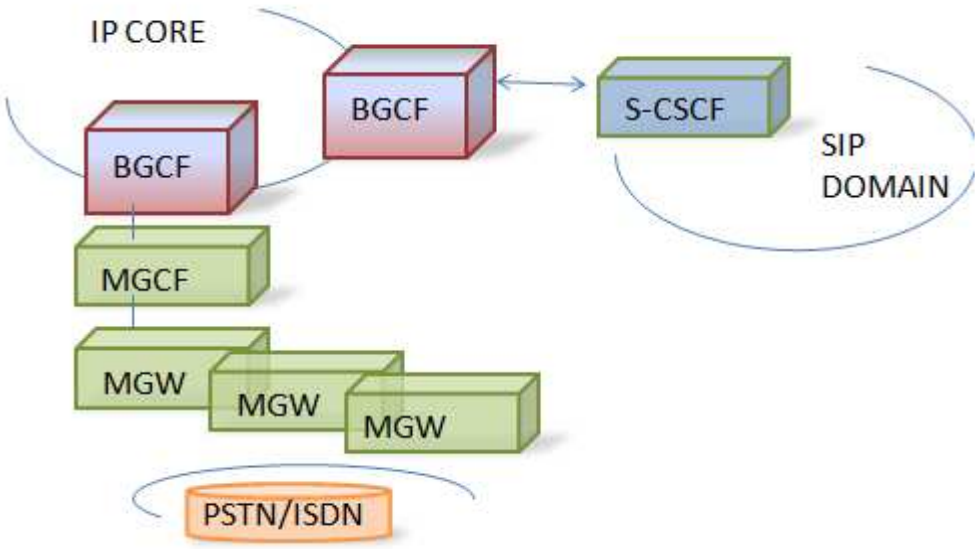


Figura 8.Estructura BGCF-MGCF

5.2.1.6. BCF

La función BCF permite a los usuarios conectados a otras redes la posibilidad de ejecutar servicios IMS. Es un software que se implementa en el S-CSCF e interviene cuando una llamada entrante a la red se recibe de otras redes o pasarelas de otra red IMS.
Su misión es usar el HSS para determinar si el usuario que realiza la llamada pertenece al dominio IMS o no. SI pertenece al dominio IMS,se procesa el mensaje SIP (solamente peticiones INVITE SIP), y en caso contrario se descarta.

5.2.1.7. E-CSCF

La función E-CSCF puede estar implementada con cualquiera de las aplicaciones CSCF o como aplicación independiente. Generalmente se encuentra implementada con otra aplicación, y se comunica con el resto de funciones CSCF a través de señalización SIP.
Cuando el P-CSCF recibe una llamada que ha generado un usuario (SIP INVITE), se compara el número de teléfono con una lista de números de emergencia. Si es una llamada de emergencia, el P-CSCF reenvía la petición al E-CSCF. Cuando E-CSCF recibe el SIP INVITE, realiza las siguientes funciones:

- Asegurar que se proporcione la ubicación de la llamada en la cabecera. IS no es así, E-CSCF se comunica con el HSS para obtener este dato, ya que finalmente el E-CSCF proporciona los datos de número al que se llama, número que inicia la llamada, y localización del mismo.

- Normaliza el formato de número de llamada si éste es internacional.

- Enruta la llamada de emergencia hacia el nodo que sea necesario. Desde el E-CSCF no se dispara ningún tipo de servicio para el usuario ni es necesario ni el registro ni la autenticación.

5.2.1.8. Principales funcionalidades

5.2.1.8.1. Routing & Addessing

EL nodo CSCF enruta el tráfico de acuerdo con los mecanismos del estándar SIP del 3GPP y el grupo IETF.
En una red IMS, las llamadas se encaminan mediante direcciones SIP en lugar de usar los números de teléfono. De este modo los números se convierten en direcciones SIP (SIP URI) en el CSCF, que a la vez interactúa con el DNS/ENUM para ello. AL mismo tiempo, el CSCF es direccionado utilizando peticiones SIP, 'SIP REQUEST URI'. El CSCSF recibe una petición SIP, 'SIP INVITE' que contiene el campo 'user = número de teléfono'; o una petición URI, 'Tel URI', y los números se traducen a SIP URI's en el CSCF.

5.2.1.8.2. Autenticación

La Autenticación en la red, permite asegurar que el usuario que intenta acceder está autorizado para hacerlo. Se realiza basándose en los esquemas del protocolo Digest para la autenticación definidos en las RFC 3261 y 2617 del IETF, que permite establecer esta función para acceso fijo o móvil. Consiste en una 'password' establecida para el acceso a red.

Cuando el S-CSCF recibe el mensaje de petición de atenticación, se envía al HSS mediante DIAMETER un mensaje que contenga una determinada credencial que el HSS procesa y determina si la credencial es válida o no. Entonces el HSS le comunica al S-CSCF si la petición debe ser aceptada o denegada.
Después de la autenticación inicial en la fase de registro, no se lleva a cabo ningún mecanismo más durante la duración de la sesión, salvo comprobar la dirección IP del usuario en el CSCF periódicamente.

A partir de la autenticación en la fase de registro del usuario, la señalización que se genere a partir de ese momento utilizará información de esa petición inicial. Si en algún momento el CSCF determina que la autenticación de la señalización del tráfico no es segura, reautenticaría al usuario empleando el mecanismo DIGEST de nuevo.

5.2.1.8.3. Seguridad de acceso SSO

El sistema SSO ("*Single Sign On*") en un método de autenticación IMS, que permite el acceso móvil y se basa en el concepto 'Entidad de Sesión' que guarda la autenticación de un usuario durante toda la sesión en la red.
En primer lugar se autentica el usuario con una dirección IP de acceso que se empleará para verificar el estado de autenticación del usuario en los servidores de acceso de la red. Estos servidores garantizan que la dirección IP en el HSS es válida. La sesión SSO puede terminar cuando el HSS inicia una petición de actualización del perfil del usuario hacia el S-CSCF, anulando la dirección IP autenticada anteriormente.

5.2.1.8.4. Registro del usuario

La función de registro permite al usuario registrarse o anular un registro con la red, y es un requerimiento básico para que el usuario pueda enviar o recibir sesiones SIP, así como simplemente el envío y recepción de peticiones SIP.
La función permite al operador autorizar o no el registro del usuario en la red y determinar a qué tipo de servicios puede acceder.
Cuando se quiere terminar con el registro de un usuario, el proceso puede ser iniciado tanto por el usuario como por la red. El usuario puede anular el registro de cualquiera de sus contactos registrados o de todos a la vez. Una Identidad Pública de Usuario es 100% anulada del registro cuando el último contacto que anula su registro no se encuentra en la red.
Cada usuario tiene una Identidad Privada de Usuario y una o varias Identidades Públicas de Usuario. Cada Identidad Púbilca puede ser registrada por varios UE, lo que permite que más de una dirección de contacto estén conectadas a la misma Identidad de Usuario Pública. Cada usuario se conecta a una subscipción que puede dar servicio a varios usuarios, pero el concepto de registro, se aplica para una dirección de contacto en concreto y una o varias Identidades Públicas de Usuario.
El registro es una operación muy común en mecanismos SIP, y es la única manera de que el sistema conozca la posición actual de un usuario. Durante el proceso, los usuarios envían peticiones de registro SIP (SIP REGISTER) hacia el Dominio de la red.

Por otro lado, también es posible que la red inicie la finalización de registro de un usuario. Anular un registro es un proceso que pretende borrar los contactos del S-CSCF de un usuario actualmente registrado en la red. Puede comenzar por razones de administración de la red o por sobrepasar el máximo tiempo de registro permitido en el S-CSCF. Cuando se produce por temas administrativos de la red, la fase de anulación del registro se dispara en el CSCF y el usuario y toda su información asociada se borra de la Identidad Pública de Usuario. El cliente no es notificado de esta acción.

5.2.1.8.5. Llamada de emergencia

Cuando se detecta una llamada de emergencia, se redirige hacia el PSAP (Public Answering Safety Point) que toma la información de localización de un usuario y el tipo de número de emergencia.

EL P-CSCF es el nodo que detecta este tipo de llamada SIP y la dirige al nodo E-CSCF. Una vez allí, el E-CSCF selecciona el PSAP entre los disponibles en la base de datos RDF/LRF mediante HTTP/SOAP/XML. Cuando se ha identificado el PSAP, entonces E-CSCF envía la llamada a través del BGCF hacia el MGC correspondiente.

Tan pronto como se detecta que la llamada es de emergencia (se compara la petición 'Request URI' con una base de datos interna del P-CSCF), el sistema IMS proporciona prioridad a través de la red. Cada nodo IMS aplicará prioridad de emergencia a esta llamada(en el nodo CSCF, el parámetro de prioridad quedaría <priority = emergency > en la cabecera de los mensajes SIP INVITE) tanto para el plano de señalización como el de media.

5.2.1.8.6. Interfaces y Protocolos

En la siguiente figura, se aprecian los interfaces y arquitectura lógica del nodo CSCF

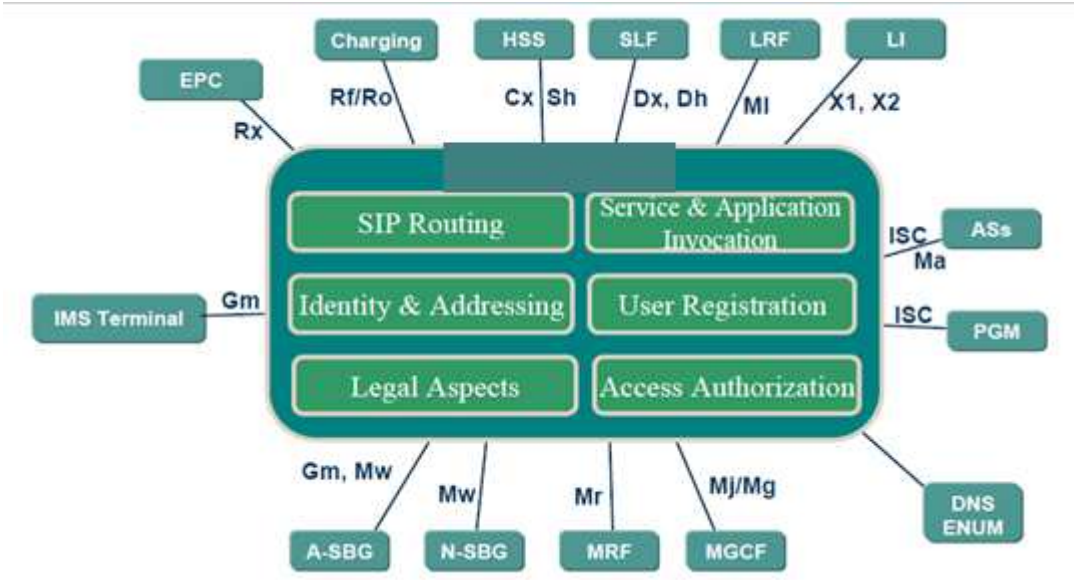


Figura 9. Interfaces y arquitectura lógica del nodo CSCF

Cada interfaz representa la comunicación entre el nodo CSCF y otros nodos de la red. Como se muestra en la tabla, se utilizan los protocolos adecuados para cada interfaz.

Tabla 4.Interfaces CSCF

Tráfico -Interfaz	Protocolo
CSCF-MRF: Ma,Mr	SIP / UDP o TCP
CSCF-CSCF: Mw	SIP / UDP o TCP
CSCF-AS: ISC	ISC (SIP) / UDP o TCP
CSCF-HSS: Cx,Sh	Diameter / TCP
CSCF-SLF: Dx,Dh	Diameter / TCP
CSCF-UE: Gm, XDM-PRS-1/2	SIP / UDP o TCP
CSCF – CDF: Rf	Diameter / TCP

5.2.2. HSS

El HSS *("Home Subscriber Server*") es la principal base de datos para los usuarios de la red y el principal punto de referencia para ofrecer seguridad de acceso, autorización, identificación de usuarios y subscripción. Este nodo almacena la información del perfil de cada ususario, es decir, los servicios que tenga asociados y la información de seguridad para el control de acceso a red.

En la red pueden existir varios HSS, por lo que en este caso, cuando la red necesite la información de un determinado usuario tendría que hacer uso del nodo SLF (Subscription Location Function), que se encarga de redirigir la petición de registro hacia el HSS que contenga la información del usuario que se desea verificar.
Durante la fase de registro, el HSS ofrece los datos del usuario para validar la autenticación del mismo, además de proporcionarle al I-CSCF la dirección del S-CSCF al que debe reencaminar las peticiones de ese usuario.

Actualmente, los usuarios abonados a redes de conmutación de paquetes o circuitos, como GSM o GPRS, tienen sus datos almacenados en el HLR y AuC . Si a su vez ese usuario dispone de capacidad IMS, tendrá los datos y el perfil asociado a IMS en el HSS correspondiente. En 3GPP, se define el nodo HSS como la base de datos común tanto para IMS como redes de conmutación de circuitos o paquetes, tomando el HLR y AuC como un subconjunto perteneciente al nodo HSS.

5.2.2.1. Perfil de usuario

En el interior del nodo HSS, se almacena el perfil asociado a un usuario y el MSISDN (Mobile Station Integrated Service Digital Network) del mismo. También garantiza que la provisión del MSISDN sea única en el nodo. EL perfil cargado y guardado en el HSS como nivel de usuario es información que más tarde se envía al CSCF.
EL HSS también dispone de una funcionalidad de Registro, que permite a los usuarios registrarse o anular un registro con tal de especificar al menos una del conjunto de identidades del que se dispone para un usuario. Al usuario de le informa del resto de

datos asociados a su petición de registro por si fuese necesario más adelante durante la sesión.

5.2.2.2. Seguridad del usuario IMS

El HSS permite emplear procedimientos de autenticación basados en los protocolos de IETF, OMA y 3GPP para el acceso con terminales SIP y acceso a los servicios a través de XCAP (XLM Configuration Aplication Protocol). Se emplea DIgest como mecanismo de autenticación de usuarios a través de terminales SIP y XCAP.

La autenticación con DIgest se basa en el mecanismo de petición-respuesta. En general, el mecanismo comienza en el S-CSCF, cuando recibe la petición SIP de un usuario. Entonces el HSS verifica la respuesta a esta petición y envía el resultado de la autenticación al CSCF. También realiza una actualización de datos del S-CSCF con la información relevante. Además, de acuerdo con el estándar 3GPP, los AS pueden leer información del usuario en el HSS a través del punto de referencia Sh.

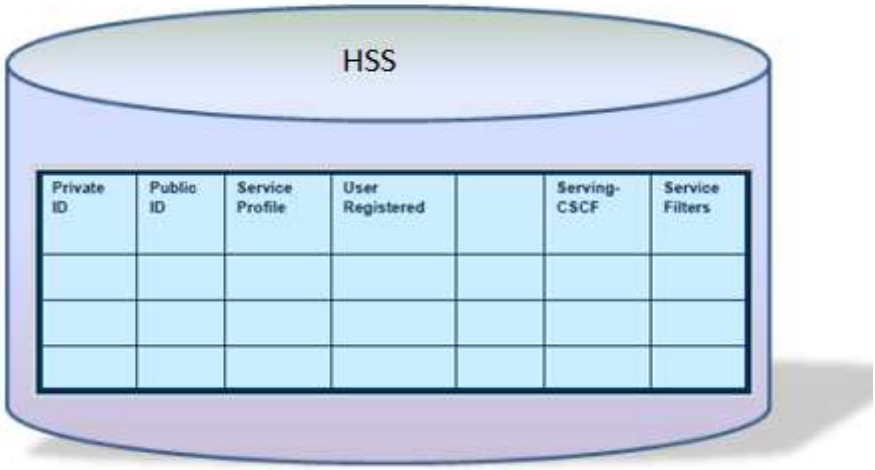


Figura 10. Datos representativos que almacena el nodo HSS.

5.2.2.3. Interfaces

El nodo HSS tiene un rol central en las redes de acceso WCDMA, GPRS, CDMA2000 y WLAN. Es empleado para tareas de control y no para procesar tráfico. Según la arquitectura 3GPP el HSS soporta los puntos de referencia Sh y Cx.

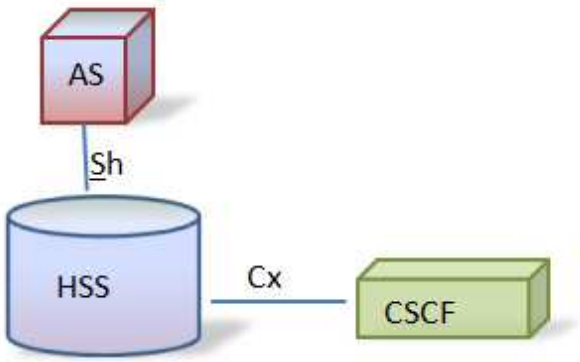


Figura 11. Interfaces Sh y Cx del HSS

El punto de referencia Cx entre el HSS y el CSCF se basa en el protocolo Diameter y soporta los siguientes procesos:

- Intercambio de información de seguridad. La información del perfil de usuario se comparte para las tareas de autenticación y autorización del acceso a los servicios IMS
- Soporte el S-CSCF en la cancelación de registro de usuario
- Recuperación de datos de localización del S-CSCF de la sesión para el I-CSCF.

Para el punto de referencia Sh entre el HSS y la capa de servicios de aplicación el protocolo empleado también es Diameter

- Recuperación de los datos del usuario y de aplicaciones IMS desde los AS.
- Para informar sobre nuevos cambios en los datos de aplicación o los usuarios.

El punto de referencia Zx implementado por Ericsson, entre un servidor de Agregación Proxy y el HSS se basa en Diameter.
Otro de los puntos de referencia que encontramos es el que se encuentra entre el HSS y el GGSN, basado en el protocolo RADIUS. Soporta autenticación SSO.

Tabla 5. Interfaces del HSS

Interfaz	Tráfico	Protocolo
Cx	HSS -CSCF	DIAMETER
Sh	HSS - AS	DIAMETER
Zx	HSS – Agragation Proxy	DIAMENTER

5.2.2.4. Protocolos

Los protocolos empleados en las comunicaciones del nodo HSS se aprecian en la siguiente figura:

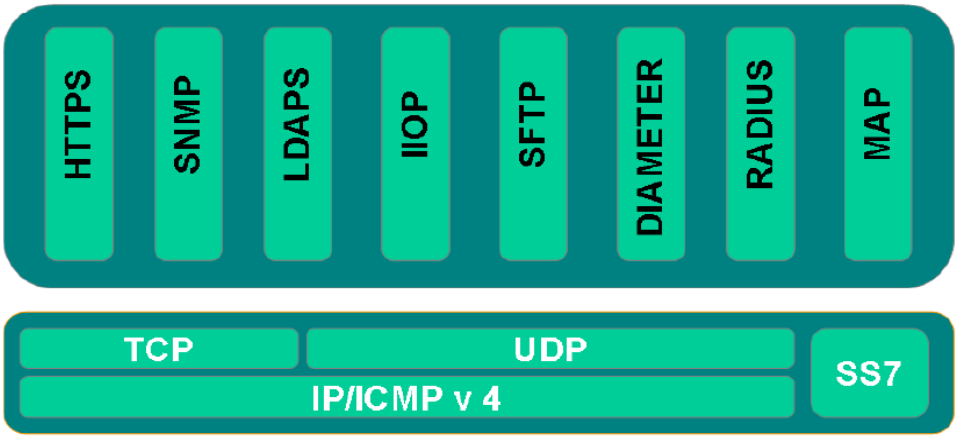


Figura 12. Componentes protocolarios en la arquitectura del nodo HSS.

- Diameter

El protocolo Diameter proporciona los servicios de autenticación, autorización y contabilidad. Es aplicable sobre TCP/IP. Más adelante veremos los mensajes que se intercambian nodos de la red IMS con el HSS basándose en este protocolo.

- HTTPS

EL protocolo de comunicanión "*Secure Hypertext Transfer Protocol*" está diseñado para transferir información encriptada entre ordenadores sore www. HTTPS es HTTP usando La capa segura SSL. HSS soporta HTTPS para operaciones y mantenimiento de clientes. Además, el nodo TSP Toolbox es accesible a través de HTTPS.

- IIOP

El protocolo de interoperabilidad de internet, "*Internet Inter-operability Protocol*" es soportado por este nodo como define el grupo IETF para las aplicaciones icluidas en el toolbox del TSP, como las funciones de notificación de funcionamiento y alarmas.

- LDAPS

AL igual que IIOP, el protocolo LDAPS está definido por el IETF y es soportado por el HSS para proporcionar la opción de lectura y escritura para la interacción y el acceso a los distintos directorios del nodo.

- SFTP

El protocolo "*Secure FIle Transport protocol*" definido por el grupo IETF permite la transferencia de datos desde y hacia el HSS. Puede ser empleado para recuperar información o acceder a software remoto para realizar actualizaciones en el nodo.

- SNMP

Este protocolo, "*Simple Network Management Protocol*" permite la gestión de la información de los elementos de red que son sometidos a una alteración en la información cuando se registra por ejemplo un usuario.
El HSS soporta las versiones SNMPv2 para la gestión de errores y SNMPv3 para la gestión del funcionamiento.

5.2.2.5. Arquitectura del nodo

La principal característica de la arquitectura del HSS es su división modular, permitiendo introducir de manera muy sencilla nuevas funcionalidades o especificaciones que un operador necesite. De esta forma se mantienen de manera independiente bases de datos para IMS o para WLAN, permitiendo cubrir múltiples escenarios y necesidades de capacidad del nodo.
En la siguiente figura puede apreciarse la modularidad que forma el HSS:

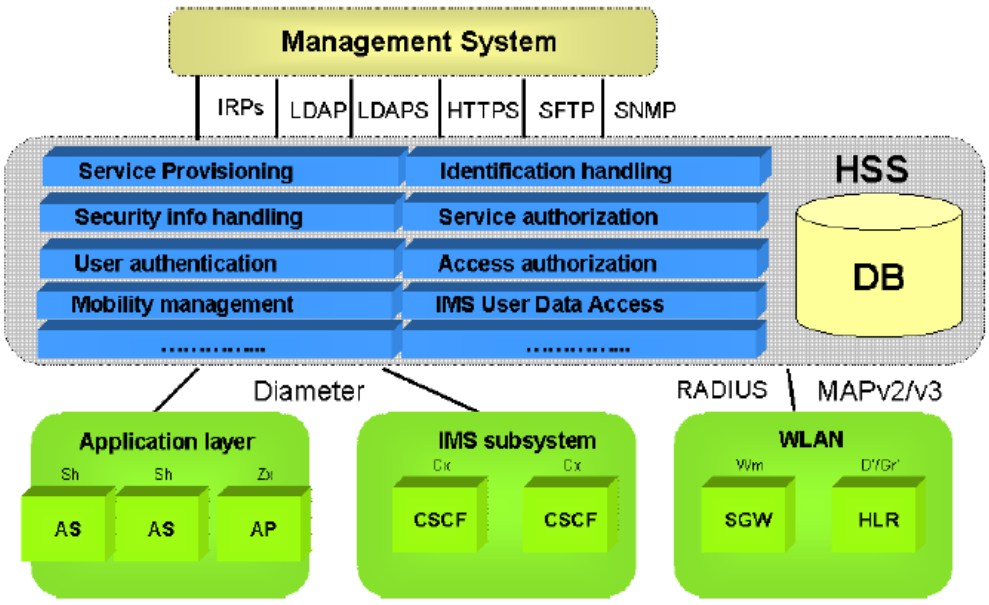


Figura 13. Modularidad funcional del HSS

para acceder a los datos almacenados en el HSS, existe una función con mecanismo de autenticación y autorización que permite que cada usuario que quiera acceder a los

datos, sea sometido a una petición de identificación por un proceso de registro mediante '*password'.* Cada usuario tendrá los privilegios que le permita su rol de perfil de usuario almacenado en el HSS.

Cuando se dimensiona la capacidad de un HSS es esencial conocer la capacidad que puede tener la red y el riesgo que existe al exceder un cierto límite. El nodo debe soportar tanto las horas con mayor tráfico como un momento de carga máxima puntual.

La capacidad del nodo dependerá del comportamiento de los usuarios subscritos, los servicios a los que tendrán acceso y el diseño de la red.

5.2.3. PSTN / CS Gateway

La pasarela PSTN proporciona un interfaz hacia la red de conmutación de circuitos. De esta forma los terminales IMS pueden recibir y realizar llamadas con cualquier otra red. Este nodo está formado por las siguientes funciones:

5.2.3.1. SGW

El Signaling Gateway establece la comunicación con el plano de señalización de la red de conmutación. Realiza la conversión de protocolos entre ISUP/MTP o BICC/MTP a ISUP o BICC sobre SCTP/IP.

5.2.3.2. MGW

El MGW es el encargado de la comunicación en el plano de datos con la red de conmutación. Es capaz de enviar y recibir datos mediante el protocolo RTP. Además, realiza la trasncodificación de datos cuando el terminal IMS no soporta la codificación empleada en el dominio de la red de conmutación. Uno de los escenarios más comunes ocurre cuando la red IMS emplea el códec AMR (3GPP TS 26.071) y en la red conmutada el G.711 de la recomendación ITU-T.

5.2.3.3. MGC

El nodo MGC (Media Gateway Controller) es un sistema flexible que puede ser integrado en distintos tipos de solución y adaptarse a las necesidades de los operadores o de los usuarios finales. Gracias al uso de estándares abiertos y los protocolos SIP, ISUP, RTSP y H.248 es posible crear distintas soluciones adaptadas a diferentes necesidades.

El MGC proporciona la función de señalización en la interconexión con las redes de conmutación de circuitos y de conmutación de paquetes. Adapta la señalización entre las dos redes y controla a los nodos MG (Media Gateway), necesarios para establecer la comunicación entre la red IMS y las de conmutación.
El MG es el responsable de manejar la información recibida desde la red de conmutación. Todas estas redes terminan en un MG cuya función principal es adaptar la información que se quiere transmitir al formato necesario para ser transportada sobre una red IP.

5.2.3.4. Interworking entre los protocolos de señalización

- Interfuncionalidad ISUP – SIP para VoIP

El MGC, implementa la función MGCF (Media Gateway Controller Function) sobre la pasarela del PSTN de la red de conmutación, para garantizar la interoperabilidad entre ambas redes. Esta función, proporciona la conversión entre los protocolos de señalización empleados en la GSTN y los protocolos de control de sesión de las redes IP Multimedia.

El MGC, proporciona los puntos de referencia Mg y Mj basados en SIP para la señalización de las llamadas y el punto Mn basado en el protocolo H.248 para el control de los medios de comunicación de los recursos en el MGW. El protocolo de señalización soportado hacia la red GSTN es ISUP. La interoperabilidad entre ISUP y SIP soportada en este nodo viene definida en la recomendación ITU-T Q.1912.5
Como se puede apreciar en la figura 20 el MGC soporta SGW separadas , pero también puede implementar la función SGW de manera integrada donde lo enlaces de señalización física SS7 ISUP/MTP terminan en el mismo nodo, MGC.

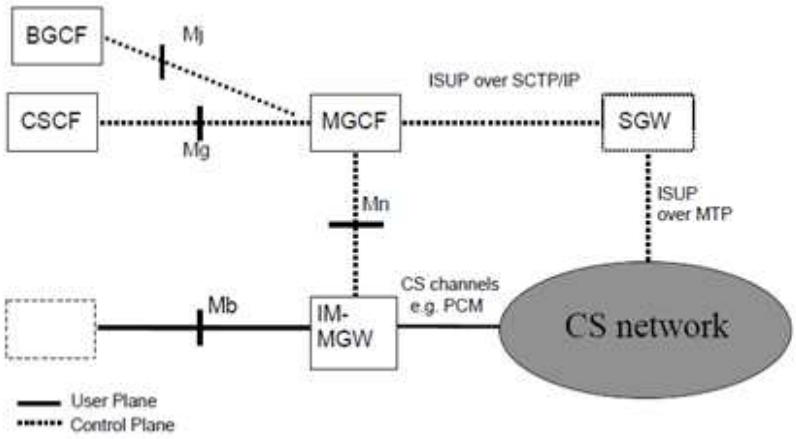


Figura 14. Nodo MGC en la arquitectura IMS

A continuación veremos los distintos tipos de tráfico que se establecen en esta comunicación:

- Conexión ISUP-ISUP entre dos nodos MGC usando SIP para VoIP:

Se trata de una combinación de llamadas de ISUP a SIP y de SIP a ISUP. La llamada ISUP de la red de conmutación de circuitos es convertida en una llamada SIP de VoIP en una pasarela PSTN y volverá a ser una llamada ISUP en otra pasarela PSTN. Este caso puede darse por las siguientes razones:

-Un servidor SIP proxy externo, como por ejemplo el CSCF, toma las decisiones de encaminamiento y enruta las llamadas SIP desde un MGC hasta otro MGC.

-Un servidor ENUM que mapea un número de llamada E.164 recibido desde una red GSTN hacia un SIP URL que devuelve esta llamada a la red GSTN por medio de otro nodo MGC.

-El número interno de análisis y configuración de datos del MGC está mapeando un número de llamada E.164 recibido de la red GSTN y dirigéndolo a un SIP URI que devuelve la llamada.

-La redirección 3XX SIP se ha establecido en el MGC y se recibe una respuesta SIP 3XX con SIP URL que es redirecciona la llamada de vuelta a la red GSTN por medio de otro nodo MGC.

- Llamada ISUP-ISUP con truncado VoIP controlado por un nodo MGC

Este caso permite al MGC controlar una conexión VoIP entre dos MG para el truncado de aplicaciones VoIP.

La llamada ISUP es recibida desde la red GSTN por un MGW que se conecta a la ruta de entrada desde la GSTN. El nodo MGC, utiliza el Called Number para seleccionar

una ruta de salida hacia el GSTN que típicamente está conectada a otra MGW que el del tráfico entrante. El MGC inicia una llamada que sale a través de la ruta de llamadas salientes y controla los dos MGs para manejar la conexión VoIP de las rutas de entrada y salida a la GSTN.

En un caso especial, si las rutas de entrada y salida están conectados al mismo MGW, el MGC se trata de la misma manera como si dos MCs fueran utilizados

La única diferencia entre este caso y otro en el que existan dos MGs es que los paquetes RTP de VoIP deben ser enrutados en un mismo MG y no en el Backbone de IP como en el caso de los dos MGs.

- Funcionamiento entre ISUP y H.323 para servicio VoIP

El nodo MGC soporta llamadas VoIP de H.323 tanto sobre H.248 como con MGCP (para guardar compatibilidad con versiones de productos anteriores que utilizaban versiones que sólo soporta MGCP)

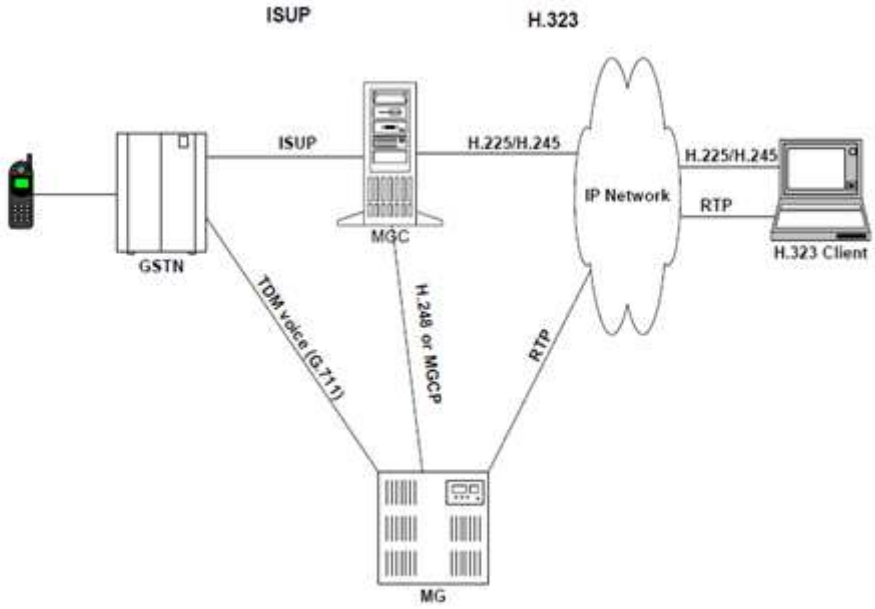


Figura 15. Configuración de interoperabilidad entre ISUP y H.323 para el nodo MGC.

Los casos de tráfico que pueden darse en esta situación son:

-Llamada de ISUP a H.323 o de H.323 a ISUP

-Llamada de emergencia de ISUP a H.323

-Truncado de llamada de ISUP a ISUP sobre IP empleando H.323

5.2.4. Funciones comunes del MGC

5.2.4.1.1. Number Analysis y Routing

'Number Analysis' es la función que analiza los números E.164 que llegan de las rutas entrantes al nodo y decide dónde debe ser enviada la llamada y con qué tipo de servicio. De este modo, identifica el perfil del servicio de cada llamada independientemente de la ruta de entrada, es decir, desde la GSTN, o desde la ruta SIP o H.323. Así, el mismo número E.164 puede ser analizado adecuadamente dependiendo de la ruta de entrada por la cual se haya recibido. En función de la ruta de entrada, se aplican distintas reglas de análisis adaptadas a GSTN o bien a SIP y H.323

Existen distintos procesos de 'Number Analysis', denominados 'A-number' y 'B-number'.

- A-Number Analysis

Se trata de una función opcional, de tal forma que si el operador no configura A-number en el nodo MGC, el análisis se hará directamente con B-Number .

Existe una primera fase, denominada preanálisis, que eanaliza el origen y el tipo de A-número de entrada utilizando la información que contienen unas tablas (tabla de preanálisis A-number) (SNMP MIB object)

Los datos obtenidos de la fase de preanálisis, son la entrada a la función de análisis A-number. Aquí se compara el número recibido, con los datos correspondientes a las tablas A-number SNMP MIB del operador. Este número puede ser modificado durante el análisis, ya sea añadiendo o quitando algún dígito, o introduciendo alguna modificación en el valor NAI (Nature of address indicator). Los datos de salida de esta función, son los de entrada para el preanális de B-Number.

Es posible anular llamadas tanto en la fase de preanálisis como en la de análisis A-Number. El operador define valores Q.850 como resultado de estas fases de análisis y son mapeados con otros protocolos como por ejemplo SIP, en los interfaces del MGC.

- B-Number Analysis

Como en la fase de análisis de A-Number, distinguimos otras dos fases en el análisis de número B, el preanálisis B-Number y análisis B-Number.

Es la fase de preanálsis, se analiza el origen y el tipo de número (parámetro Called Party Number) ytilizando los datos de configuración definidos en las tablas SNMP

MIB. Cuando se completa el preanálisis los datos de salida constiuyen los de entrada para la faase de análisis. Es esta fase se compara, aligual que con el A-Number, dígito a dígito la cadena recibida con la definida en las tablas del operador. La información de salida de esta fase es empleada como referencia para las tablas de enrutamiento del operador.

Con esto, es posible seleccionar un MG que soporte las especificaciones de enrutamiento y buscar caminos alternativos si alguna de las rutas no está disponible en un determinado momento. Existe otra función que emplea el MGC denominada FAR (Fixed Alternative Routing) que se emplea para direccionar las llamadas a través de diferentes rutas en cada momento determinado con el objetivo de seleccionar la ruta más óptima disponible en cada momento basándose en las estimaciones de tráfico y coste que establece el operador según el día y la franja horaria.

5.2.4.2. Función de autenticación, autorización y tarificación (AAA)

EL nodo MGC implementa esta función haciendo uso del protocolo RADIUS. Tiene como objetivo apoyar la GSTN para contabilizar correctamente en la interconexión de distintas redes. Esto permite a los operadores utilizar servidores RADIUS para autorizar y contabilizar los números (A-Numbers) de GSTN que son permitidos.

La autenticación y la contabilidad son tratados y configurados independientemente dentro del nodo, por lo que es posible implementar sólo una de ellas o las dos funciones a la vez según las necesidades del diseño. El MGC es capaz de comunicarse con otros servidores de autenticación y facturación con tal de establecer redundancia a la aplicación. El nodo también implementa un buffer de almacenamiento (no volátil) para almacenar información a contabilizar si en un instante no están disponibles los servidores.

La base de datos que dimensiona la cantidad de llamadas en cada instante decide el timepo máximo en el que el MGC puede almacenar cierta información en el buffer. EL nodo envía los datos a contabilizar desde el buffer hacia los servidores mediante RADIUS cuando éstos están disponibles.

Este nodo ejecuta la función AAA basándose principalmente en la información de señalización de la llamada recibida, como por ejemplo el parámetro Called Number recibido mediante ISUP.

5.2.4.3. Soporte al DNS

EL MGC es capaz de comunicarse con servidores DNS externos con tal de ofrecer las siguientes funcionalidades:

- Soporte a ENUM mediante *DNS NAPTR records*
- Búsqueda de servidores SIP mediante *DNS SRV records*
- Convertir los nombres de dominio a direcciones IP empleando DNS *A-records.*

Para ello es necesario que los servidores DNS con los que se comunica el MGC tengan configurada la función de gestión de configuración del MGC, 'MGC Configuration Management Function'.

Para definir en el MGC las direcciones IP de éstos DNS es posible definir directamente la dirección del DNS primario y del secundario sobre el MGC, o que el operador establezca una plataforma de configuración donde el MGC puede tomar la dirección de los DNS establecidos en una lista (el primer servidor se toma como el primario). Cuando el MGC envía la petición al DNS primario, espera durante 2s la respuesta, y en caso de no recibirla, la petición será enviada al DNS secundario. Si éste agota otros 2s sin respuesta, la llamada afectada será rechazada.

Si en un nodo MGC no se permite implementar la comunicación con el servidor DNS, se reduce la funcionalidad del mismo. Este modelo, podría utilizarse si el soporte ENUM no se utiliza y si todas las direcciones IP de los nodos adyacentes se definen directamente en la configuración del nodo MGC en lugar de los nombres de dominio.

5.2.5. DNS / ENUM

En IMS se permite la identificación de los nombres de la red mediante un nombre de dominio que estará asociado a una dirección IP. Para llevar a cabo el enrutamiento, será necesario emplear la función de DNS ("*Domain Name Server*") para obtener la dirección IP asociada al nombre de dominio.

DNS hace que una red sean más fácil de usar y gestionar al proporcionar una correlación entre una dirección de red y el nombre de dominio.

También permite que la red administradora pueda ocultar los detalles acerca de cómo se implementa un servicio detrás de un nombre de dominio.

Existe otra funcionalidad, denominada ENUM que se puede implementar en los DNS, y permite disponer en el DNS de entradas con formato E.164. Para estos casos, ENUM permite traducir el número de teléfono a una SIP-URI y poder realizar el enrutamiento de mensajes SIP, ya que es imprescindible la SIP-URI para ello.

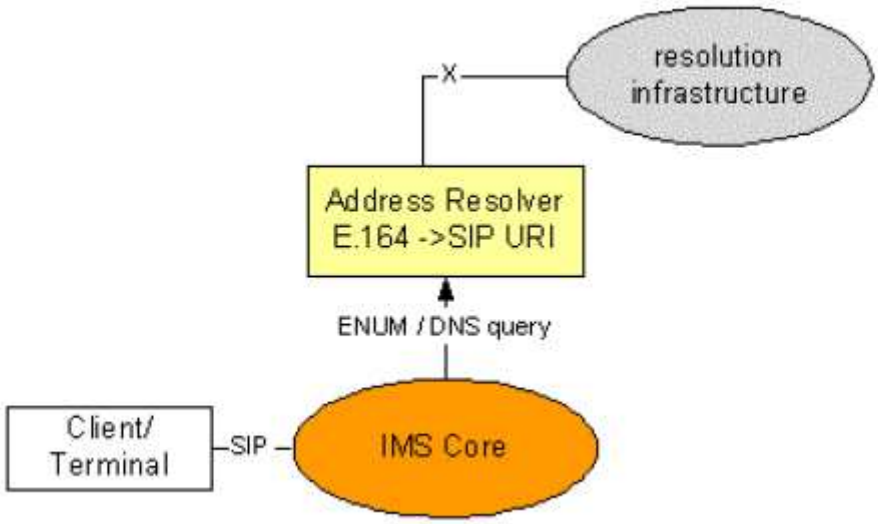


Figura 16. Arquitectura de resolución de nombres de dominio

Por otro lado, encontramos también los servidores DHCP ("*Dynamic Host Configuration Protocol")*. DHCP es un protocolo de red de la forma cliente/servidor y que ofrece a los clientes de una red IP poder obtener sus parámetros de configuración. Toda la información relacionada está publicada en la RFC 2131 para DHCP y en la RFC 3315 para DHCPv6

DHCP soporta tres mecanismos distintos para la asignación de direcciones IP:

• Asignación automática: DHCP asigna una dirección IP permanente elegida por el servidor DHCP para un cliente.
• Asignación dinámica: DHCP asigna una dirección IP a un cliente por un período concreto de tiempo (o hasta que el cliente renuncia expresa a la dirección).
• Asignación manual: el administrador de la red asigna la dirección IP del cliente,y DHCP se utiliza simplemente para transmitir la dirección asignada al cliente.

5.2.6. SBC

El nodo SBC ("*Serial Border Controller*") o también conocido como SBG ("*Serial Border Gateway*") es el encargado de la correlación de toda la señalización y los flujos de media (como audio y vídeo) que pasa por los extremos de la red, proporcionando un conjunto completo de funciones que son necesarias para acceder e interconectar el dominio IMS con otras redes IP multimedia.

Este nodo proporciona acceso con seguridad, protección del ancho de banda, calidad del servicio, nivel de servicios acordados y otras funciones críticas para las transmisiones en tiempo real de audio o vídeo.

EL SBC se localiza en los extremos de la red, el punto de infraestructura donde una sesión pasa de una red a otra. Dentro del nodo podemos diferenciar dos partes que lo componen:

- SGC, Session Gateway Controller, que se encarga del plano de señalización
- MG, Media Gateway, que soporta el tráfico de datos.

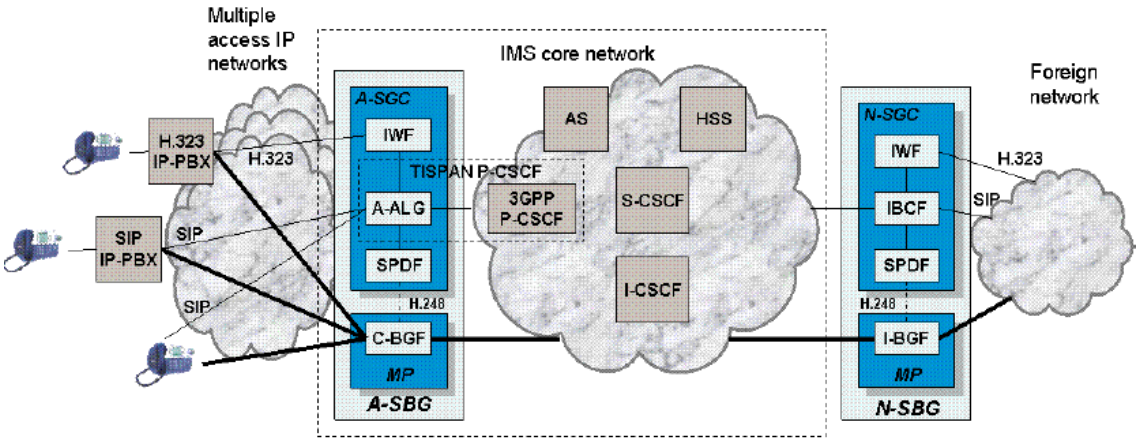


Figura 17. Roles del SBC en una red IMS

Como se muestra en la figura existen tres grandes funciones para este nodo dentro de la red:

- A-SGC: cuando la funcionalidad SBG se implementa entre la red IMS core y la red de acceso. Sólo permite el tráfico de señalización hacia y desde los usuarios que están registrados en la red central IMS (en el HSS). La excepción se produciría con llamadas de emergencia de usuarios no registrados que pueden ser aceptadas si así se configura en el nodo.

- N-SGC: funcionalidad implementada entre la red IMS core y una red externa. Puede enrutar tráfico hacia cualquier red consultando los 'DNS NAPTR records', 'SRV records' y 'A records' según indica la RFC 3263 para redes SIP.

- MP ("*Media Proxy*"): protege los nodos centrales de la red IMS de los posibles ataques y bloquea el tráfico malicioso. Dispone de alarmas están para hacer que el operador sea consciente de posibles intentos de ataque.
  Para asegurarse de que las interfaces Ethernet no se utilice excesivamente, el MP realiza un seguimiento del ancho de banda reservado para el flujo de datos. Una parte del ancho de banda está siempre reservado para llamadas de emergencia.

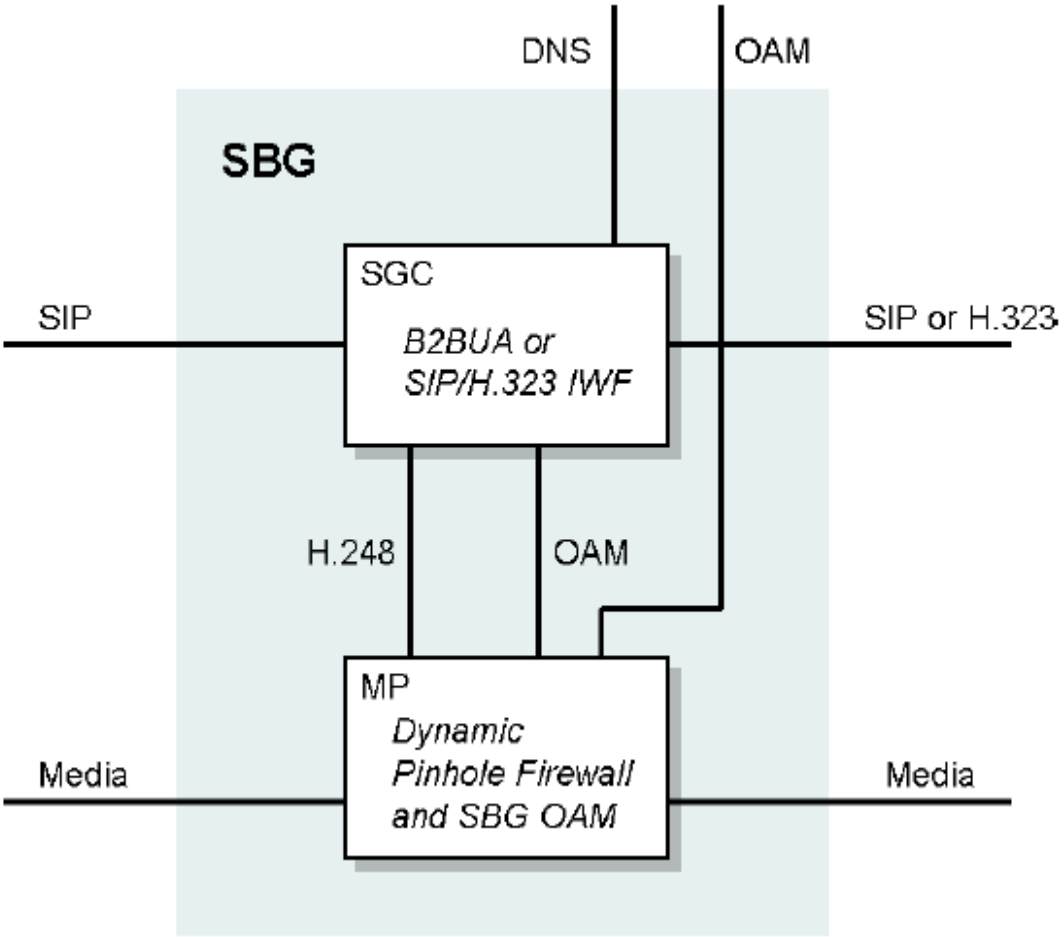


Figura 18. Lógica interna del nodo SBG

Las acciones más destacables del nodo sobre la red son:

- La protección del perímetro de la red central IMS: filtrado, protección contra sobrecarga, y la limitación de velocidad para bloquear las inundaciones de tráfico IP y proporcionar protección contra la denegación de servicio (DoS).
- Registro y alertas de ataques de red y los eventos relacionados con la seguridad
- Validación de mensajes SIP / H3.23: Control de sintaxis de mensajes. Además, A SBG-sólo acepta mensajes desde los agentes de usuario registrados o mensajes de llamadas de emergencia.
- Ocultación de identidad: no hay información sobre las direcciones IP utilizadas en el núcleo de red IMS o por los usuarios de la red de acceso y la red externa.
- Permite al operador configurar el SBG funcionalidades que implementan RTCP.
- 'Media anchoring': actualización de direcciones y puertos en el SDP para que los flujos pasen a través de SBG.
- Asegurar la QoS: control sobre el ancho de banda disponible en cada momento.
- Permite tráfico SIP/UDP o SIP/TCP
- Soporta centralitas IP-PBX tanto SIP como H.323 y reconoce el tráfico que va desde/hacia la IP-PBX y aplica un tratamiento especial en los mensajes. Puede modificar las cabeceras de los mensajes para direccionarlos correctamente.
- Acepta llamadas de emergencia incluso de usuarios ajenos a la red y prioriza las mismas tanto en el plano de señalización como en el de control.
- Adapta la señalización entre SIP y H.323 (N-SBG)
- Un SBG puede configurarse al mismo tiempo como A-SBG y N-SBG

.

5.2.7. AS

En esta sección describiremos los distintos Servidores de Aplicación, AS ("*Application Servers*") que nos encontramos en la red IMS y su principal funcionalidad.
El nodo AS proporciona la lógica (pueden comenzar, modificar y terminar una sesión) de los servicios que lleve implementados. Generalmente dentro de la red existen múltiples AS, donde cada uno suele implementar un servicio. Los AS pueden localizarse en la 'Home Network' o en redes externas, si se trata de un servicio que por

ejemplo porporciona un proveedor que haya solicitado el operador de red. Todos se caracterizan por implementar Interfaz SIP hacia el S-CSCF, conocido como ISC (*"IMS Service Control*"). Además, estos nodos pueden implementar protocolos como HTTP o WAP necesarios para las aplicaciones que desarrollan. En estos servidores, el usuario se 'registra' en la página web que ofrecen y se almacena la SIP URI. La interfaz gráfica de usuario que ofrece la página web del servidor es una mejora notable para el usuario final, a la hora de configurar un servicio si lo comparamos con los procesos de las redes de conmutación.

Otro interfaz de comunicación en el AS es el denominado como Ut basado en XCAP, que proporciona al usuario la capacidad para el manejo de grupos, listas, etc. EL protocolo XCAP define como utilizar HTTP para crear, modificar o eliminar un elemento en XML.

Existen diferentes tipos de AS:

- SIP-AS: Este AS es el primero que se estableció en la red IMS, e incluso si está alojado en la 'Home Network' es capaz de comunicarse con el nodo HSS (interfaz Sh basado en DIAMETER) de manera opcional si es necesario para la lógica que implementa obtener datos de este nodo.

- OSA-SCS: con este AS se permite obtener un interfaz de comunicación hacia el entorno de aplicación OSA desde la red IMS. Se conoce como Servidor de Mediación, ya que permite acceder a servicios de otra tecnología. Todos los servicios que se desarrollan hoy en día utilizan los servidores SIP, pero para las funcionalidades ya existentes en esta plataforma (OSA) se permite el acceso a través de estos AS.

- IM-SSF: Se trata de un servidor de mediación, que puede actuar como servidor de aplicación SIP que a la vez es capaz de comunicarse mediante el protocolo CAMEL para utilizar los servicios de las redes GSM.

Cuando los AS actúan como si de un UA se tratara, observamos en la siguiente figura, que la petición INVITE que llega desde el P-CSCF y el S-CSCF origen, se reenvían hacia el AS para que éste conteste con un mensaje SIP 200 OK y devorlverlo al terminal IMS

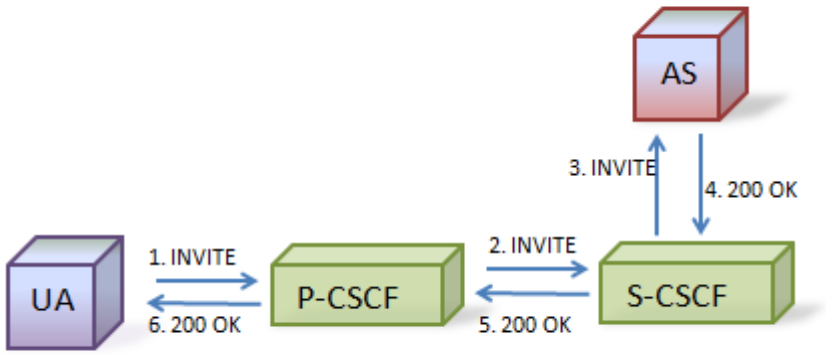


Figura 19. AS actuando como SIP UA de terminación de llamada ofreciendo servicios a un determinado usuario.

Otro caso diferente sería el mostrado a continuación en el que el AS actúe como UA ofreciendo servicios al emisor de la llamada. El UA emisor envía la petición que será recibida en el I-CSCF, y que a su vez la encamina al S-CSCF. Una vez aquí, el S-CSCF decide si debe enviar la petición a un AS. Una vez lo envía al AS, éste es el encargado de actuar como UA, estableciéndose la sesión. Responderá en tal caso con un mensaje SIP 200 OK que se reenvía de nuevo al I-CSCF pero que no llegará hasta el UA origen. Este es el modelo que se utiliza para el servicio de presencia en la red.

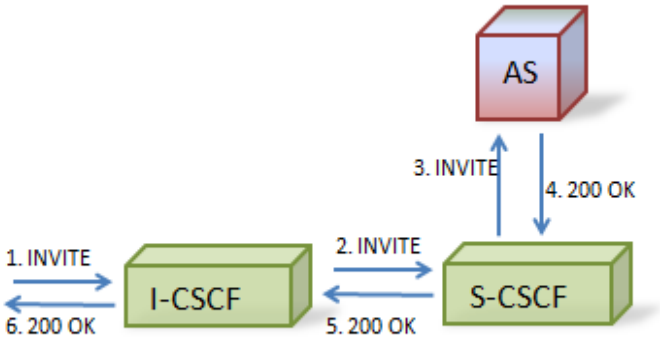


Figura 20. AS actuando como SIP UA de terminación de llamada.

Ahora veremos un ejemplo en el que el AS actúa como UA origen de la petición de sesión. El usuario directamente recibe la petición de sesión, como podría ser una aplicación de 'llamada de alerta o alarma' a un terminal.

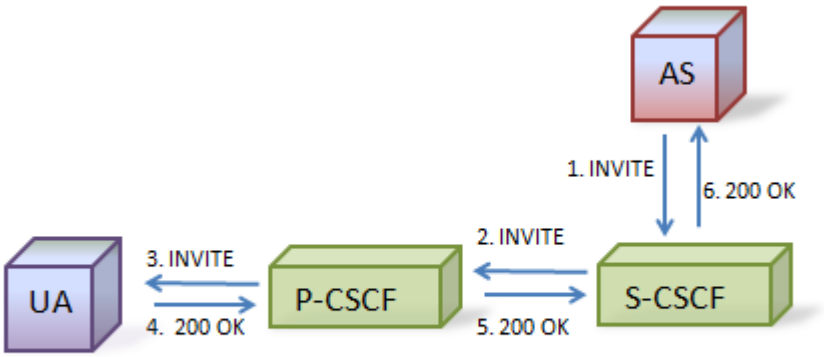


Figura 21. AS actuando como SIP UA al proveer servicios al usuario

Otra de las situaciones más comunes sucede cuando el AS actúa como servidor proxy SIP interviniendo en la llamada que genera el UA origen antes de llegar al UA destino. El terminal de IMS envía una petición que pasa por el correspondiente P-CSCF y S-CSCF. Aquí el S-CSCF decide involucrar a al AS, insertando en la cabecera de la petición la dirección del AS en primer lugar para el campo '*route*' y su propia dirección en segundo lugar para indicarle al AS dónde reenviar los mensajes de vuelta.

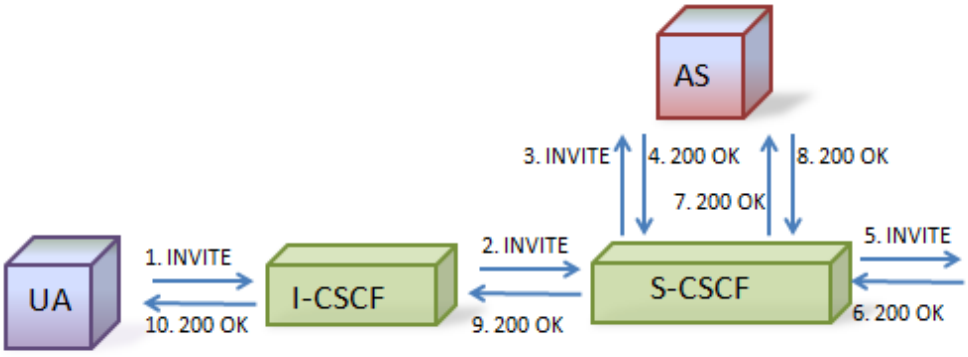


Figura 22. AS actuando como proxy SIP Server.

Existen múltiples funcionalidades y actuaciones por parte de los AS en la red, dependiendo del servicio a implementar, siendo análogo el comportamiento a los casos expuestos.

5.2.8. Media Server

El servidor media SIP es una plataforma utilizada para ofrece servicios multimedia interactivos capaces de manejar un número elevado se sesiones simultaneas en un amplio rango de configuraciones.

Se trata de un equipo que dispone de una funcionalidad llamada MRF "*Multimedia Resource Function*" y que provee interacciones entre usuarios y aplicaciones a través de recursos de voz y vídeo. Mediante el procesador MRFP "*Multimedia Resource Function Controller*" es posible desempeñar las funciones del tipo detección de tonalidad, síntesis y reconocimiento de vozl, de traducción de media, control de recursos, envío de mensajes, grabaciones, etc.

Todo el tráfico multimedia, pasa por el MRFP si tiene que atravesar la red IMS. El tráfico entrante llega a este nodo, y es encaminado hacia su destino. También permite originar flujos de tráfico, como anuncios de audio o vídeo que envíe la propia red.

Otra de las funciones que permite implementar MRFP es el control de derechos de acceso a recursos compartidos en un entorno de tráfico *'half-duplex',* donde el propio nodo es el que gestiona el control del 'token' para permitir enviar ráfagas de datos.

Con la arquitectura de IMS, es posible distribuir los servidores según la aplicación que vayan a desarrollar o disponer sólo de aquellas funcionalidades a cliente que se deseen, optimizando el coste de red para el operador.

6. Registro en la red y casos de tráfico

A continuación, se expondrán distintos escenarios de tráfico en una red IMS, contemplando diferentes posibilidades de las existentes con tal de apreciar las diferencias entre ellas.

6.1. Registro de un usuario en la red IMS

Para que un usuario acceda a la red, el primer paso es la fase de registro. Durante este proceso se activan las identidades públicas del usuario que se emplearán en las sesiones multimedia. Se realiza mediante señalización SIP y para gestionar la autorización y autenticación del usuario en la red se realiza mediante el proceso IMS AKA *(IMS Authentication and Key Agreement*). Para ello, es necesario cumplir unos requerimientos básicos a la hora de acceder a la red.

6.1.1. Requerimientos de acceso IMS

Antes de que un terminal IMS pueda acceder a dicha red, el proveedor de servicio IMS tiene que autorizar esta acción. El terminal necesita acceder a una IP-CAN (IP Connectivity Access Network) como GPRS en redes UMTS y GSM, ADSL o acceso WLAN. De esta forma, IP-CAN proporcionaría acceso a la red IMS. El prerrequisito, es el que el terminal IMS obtenga la dirección IP, típicamente dinámica, de la IP-CAN del operador.

Una vez obtenida esta dirección IP, es posible obtener la dirección del punto de entrada a la red IMS, el nodo P-CSCF. Este nodo funcionará como servidor proxy de entrada y salida, pasando por este servidor toda la señalización SIP que envíe el terminal. Este mecanismo está activo durante toda la fase de registro y típicamente se lanza el proceso cuando se enciende el terminal.

La capa IP-CAN es totalmente independiente de la capa de aplicación (SIP) de IMS. EL procedimiento de registro permite a la red IMS conocer la localización del usuario y dar lugar a la autorización del establecimiento de una sesión SIP.

6.1.2. Búsqueda del P-CSCF

Si consideramos que el terminal IMS ha accedido a la IP-CAN correspondiente y ha obtenido la dirección IP dinámica para poder lanzar la búsqueda del P-CSCF que le corresponde, se realizaría un procedimiento basado en DHCP /DHCPv6 o DNS.

El terminal envía una petición de información DHCP preguntando por las opciones DHCPv6 de los servidores SIP. En las siguientes figura y tabla se aprecia paso a paso el procedimiento a seguir.

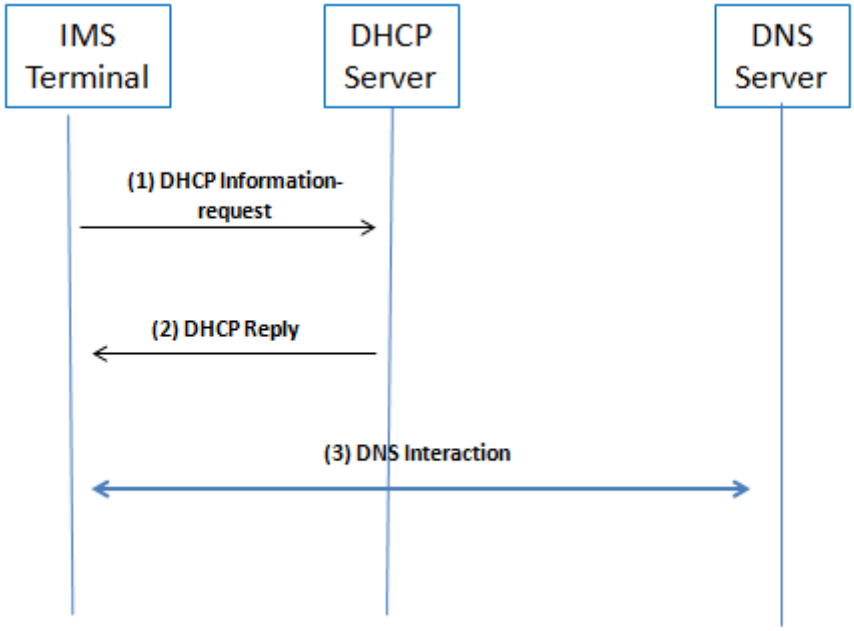


Figura 23. Flujo de datos en fase de registro.

Tabla 6. Flujo de datos en fase de registro

Número de mensaje	Descripción
1	El terminal IMS envía una petición DHCP, (DHCP Information-Request) preguntando por la lista de servidores de dominio SIP disponibles. Se marcan los siguientes campos dentro de la petición: -Option: SIP Server domain name list -Option: DNS recursive name server
2	El servidor DHCP contesta a la petición con un DHP Reply Message que contiene generalmente varios nombres de dominio o direcciones IP de distintos P-CSCF.
3	Si se reciben directamente las IP del P-CSCF el terminal IMS enviará directamente una petición SIP al nodo. En caso de recibir los nombres de dominio, será necesario hacer uso del DNS. Se iniciaría un diálogo petición-respuesta con el servidor DNS cuya dirección IP se incluía en el mensaje del servidor DHCP.
4	El DNS correspondiente resuelve la petición y devuelve el nombre de dominio del P-CSCF en una o más direcciones IPv6.

Cuando el terminal IMS obtiene la dirección IP del P-CSCF, podrá enviar señalización SIP al nodo y comenzar con el registro en el nivel IMS y el establecimiento de la sesión.

El registro en IMS es un proceso en el cual el usuario solicita autorización para acceder a los servicios que ofrece la red. Se realiza mediante petición de registro SIP (SIP REGISTER Request) El usuario envía su Identidad Pública y su Identidad Privada.

En las redes IMS; uno de los posibles procesos para la autenticación del usuario es el denominado DIGEST (RFC 2671). Se trata de una autenticación cifrada en la que el usuario y la red disponen de una clave, pero la única información que se intercambia son parámetros que junto con la clave que dispone el terminal, el usuario sería capaz de generar una nueva clave que envía a la red. La red realiza un algoritmo de comparación para comprobar si el usuario puede ser autorizado o no. Este intercambio de datos se conoce generalmente como 'desafío', y hace referencia al proceso IMS AKA. Se puede apreciar el proceso en la siguiente figura.

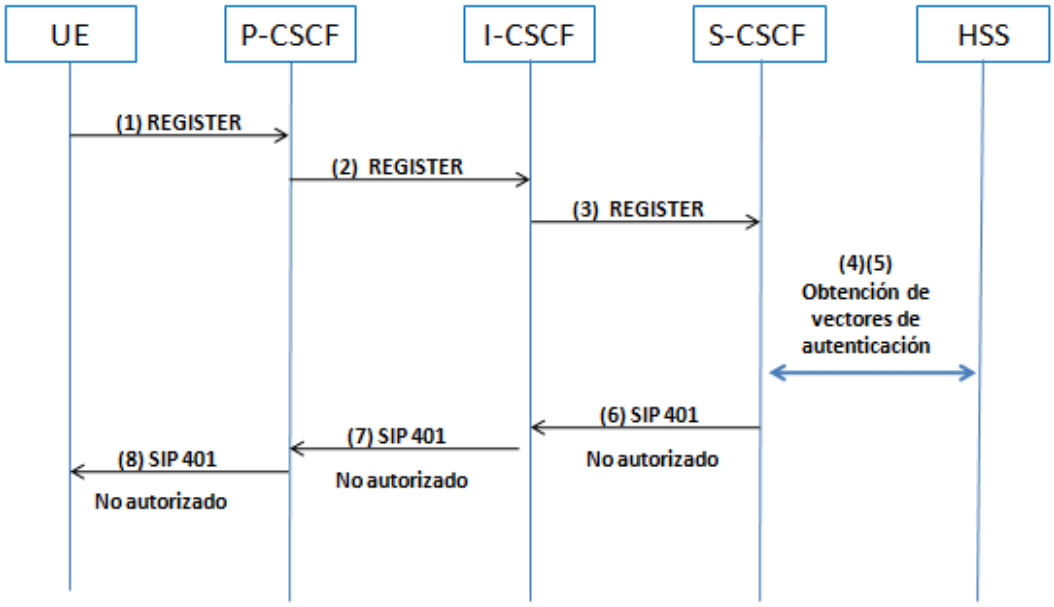


Figura 24. Procedimiento IMS-AKA

Tabla 7. Procedimiento IMS-AKA

Número de mensaje	Descripción
1	El usuario UE, envía un mensaje de registro SIP (SIP REGISTER) no protegido al P-CSCF, como registro inicial . Contiene la Identidad Privada de Usuario y las Identidades Públicas que después se quieran usar.
2	P-CSCF detecta que es un mensaje de registro inicial al no estar protegido por ningún modo de seguridad. El nodo envía un mensaje SIP (SIP REGISTER) al I-CSCF.
3	EL I-CSCF reenvía la petición de registro SIP (SIP REGISTER) al S-CSCF.
4	S-CSCF comprueba que el usuario no está registrado en la red y envía un mensaje DIAMETER al HSS para obtener los vectores de autenticación del usuario.
5	El HSS envía mediante mensaje DIAMETER los vectores de autenticación en un mensaje
6	El S-CSCF envía un mensaje SIP 401 (usuario no registrado) al I-CSCF, que contiene las claves que ha aportado el HSS para la autenticación.
7	El I-CSCF reenvía el mensaje SIP 401 al P-CSCF
8	El nodo P-CACF notifica al UE el mensaje SIP 401.

Una vez que el UE recibe el mensaje SIP 401 que contiene además de números aleatorios, la información que ha enviado el HSS para la autenticación, genera de nuevo un mensaje SIP REGISTER con la información correcta para verificar su acceso a la red. Se vuelve a generar toda la fase de registro como si del inicio se tratase, pero esta vez el HSS aportará la información necesaria del perfil del usuario.

Una vez localizado el P-CSCF, el usuario puede registrarse en la red IMS. Es importante notar que el P-CSCF puede localizarse en la misma red del usuario ('home network'), o bien en otra red ('visited network'). Generalmente, se encuentra en otra red y es necesario crear un punto de entrada a esa red vecina mediante procedimientos establecidos en la RFC 3263 que ejecuta el nodo DNS. Además el P-CSCF introduce en la cabecera del mensaje SIP URI el parámetro <P-visited-network-ID> que contiene un identificador de la red en la que se encuentra ese P-CSCF. También introduce un campo en la cabecera, <Path header> con su propia SIP URI para solicitar a la red que reenvíen a través de este P-CSCF todas las peticiones.

6.1.3. Registro en la red IMS

El registro en la red IMS es necesario antes de establecer una sesión SIP. El concepto de sesión comprende las acciones que se realizan desde que se establece un intercambio de datos entre dos usuarios y el momento en el que cesa el intercambio.
En el nivel IMS, el registro comienza con una petición de registro SIP (SIP REGISTER)
Para analizar el registro de un usuario, tendremos en cuenta las siguientes consideraciones de cara a la red IMS:

- Identidad Privada de Usuario, IMPI (*IMS Private User Identiy*): eva@ims.operador.com
- Identidad Pública de Usuario, IMPU (*IMS Public User Identity*):
  -SIP URI: eva.m@ims.operador.com
  -Tel URI: <+34600000000>

Los usuarios que no dispongan de terminal IP, se caracterizarán con el número de teléfono exclusivamente.
En la siguiente ilustración se aprecia el intercambio y la secuencia de mensajes que se llevarán a cabo y en la tabla 8 se describe el tipo de mensaje.

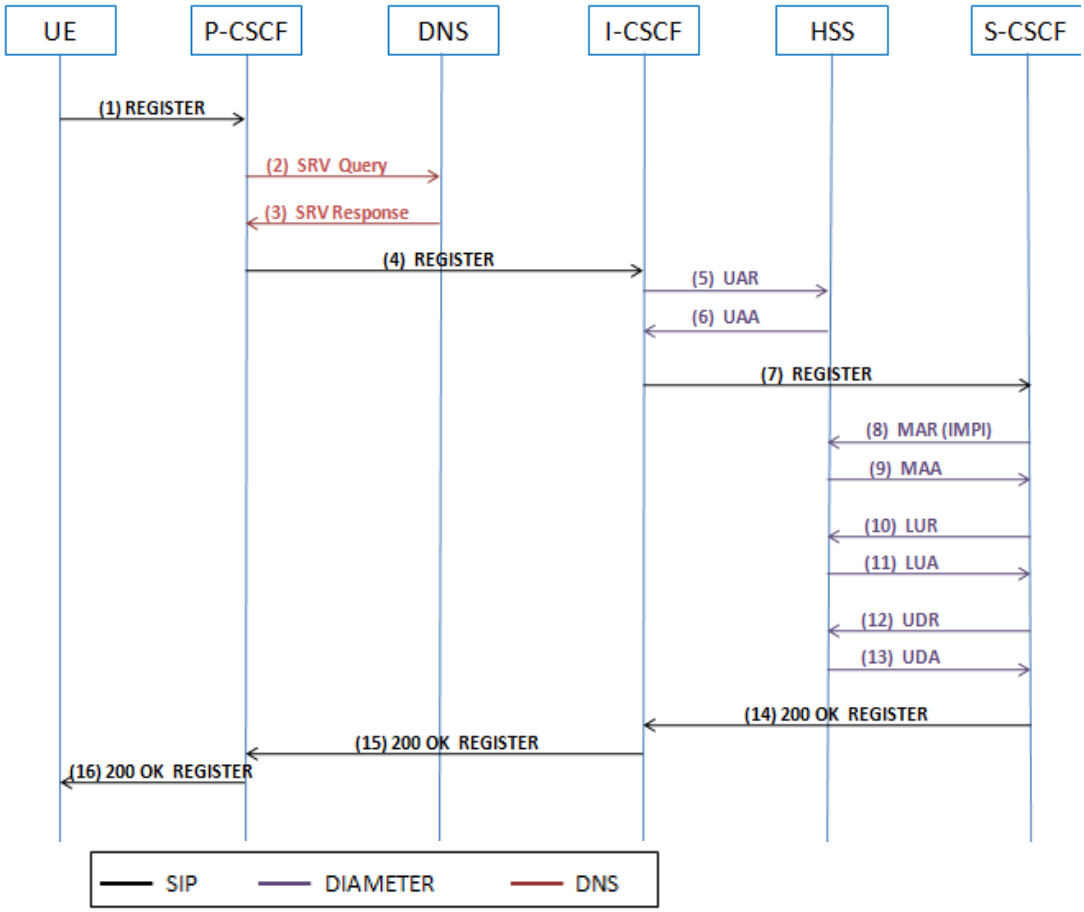


Figura 25. Procedimiento de registro en la red IMS

Tabla 8. Pasos del registro en la red IMS

Número de mensaje	Descripción
1	El usuario UE, envía un mensaje de registro SIP (SIP REGISTER) al P-CSCF.
2	P-CSCF envía un ‘ SRV Query’ al servidor DNS para encontrar el I-CSCF capaz de manejar el registro.
3	EL DNS devuelve la dirección del I-CSCF más próximo al P-CSCF que está trabajando en el registro
4	P-CSCF envía un mensaje ‘SIP REGISTER’ al nodo I-CSCF.

5	I-CSCF envía un mensaje DIAMETER que contiene una UAR (User-Auth-Request) al HSS para conseguir un S-CSCF de las capacidades que el usuario requiere.
6	HSS devuelve otro mensaje DIAMETER con una UAA (User-Auth-Answer) hacia el I-CSCF.
7	I-CSCF A busca en su table de 'fuentes' (Resource Broker table) un S-CSCF que tenga la mayor prioridad y capacidad para el usuario. La tabla está configurada para devolver el nodo S-CSCF más cercano al usuario. I-CSCF dirige el 'SIP REGISTER' hacia S-CSCF seleccionado.
8	S-CSCF envía un mensaje DIAMETER que contiene una MAR, (Multimedia-Auth-Request) (MAR) hacia el HSS para disponer de la información de autenticación del usuario.
9	HSS envía al S-CSCF una MAA (Multimedia-Auth-Answer) en mensaje DIAMETER que contiene la dirección IP del usuario (almacenada por el GGSN comop parte del procedimiento 'PDP Context Activation'.
10	S-CSCF A determina que el registro del usuario ha sido implícito, ya que la dirección IP del usuario va en el mensaje MAA. El S-CSCF almacena la dirección IP del usuario y envía al HSS un mensaje DIAMETER que contiene una LUR, (Location Update Request) para almacenar su propio nombre en el perfil de subscripción del usuario.
11	HSS responde al S-CSCF con una LUA, (Location Update Answer) mediante mensaje DIAMETER.
12	S-CSCF envía un mensaje DIAMETER con un UDR,(User Data Request) hacia el HSS para descargar el perfil de servicios del usuario.
13	HSS devuelve un UDA(User Data Answer) al S-CACF con la información de servicios del usuario.
14	

	S-CSCF envía un mensaje que contiene 200 OK (REGISTER) al I-CSCF.
15	I-CSCF envía el 200 OK (REGISTER) al P-CSCF.
16	P-CSCF envía el 200 OK (REGISTER) al usuario y éste almacena la información de la cabecera que indica la ruta de servicios (Service Route) para utilizarlo posteriormente al realizar una llamada.

Como hemos visto, el primer paso es el envío de la petición SIP al P-CSCF. En este mensaje el usuario indica quién quiere registrarse en el campo <to>, y la identidad pública a registrar en el campo <contact>. También propone el campo <expire> que contiene el valor en segundos tras el cual hay que volver a registrarse en la red, ya que la red deregistraría al usuario en caso contrario.

```
REGISTER sip:ims.Operator-X.com SIP/2.0
To: sip:eva.m@ims.operador.com
From: sip:eva.m@ims.operador.com;tag=sdfasfd
Call-ID: 2342sdfasdf
CSeq: 1 REGISTER
Via: SIP/2.0/UDP UEC_IP_address:port;branch=xyz
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD;utran-cell-id="C359A3913B20E"
Contact: <sip:UEC_IP_address:port>;expires=3600
Route: <sip:pcscfa_ip_addr:port;transport=udp;lr>
Content-Length: 0
```

Figura 26. Mensaje SIP REGISTER

A continuación, el P-CSCF envía una petición SRV al DNS para conocer la localización del I-CSCF indicando el nombre del nodo solicitado y a continuación el DNS responde al P-CSCF con una SRV-Response.

```
Queries:
      Name: _sip._UDP.icscf.asg.ims.Operator-X.net
      Type: SRV
      Class: IN
```

```
Answers:
      Name: icscf.asg.ims.Operator-X.net
      Type: A
      Class: IN
      …
      Addr: IP address of ICSCF A
```

Figura 27. Mensajes entre P-CSCF y DNS en fase de registro

De este modo el P-CSCF consigue la dirección del I-CSCF y procede a enviar una petición de registro

```
REGISTER sip:ims.Operator-X.com SIP/2.0
To: sip:eva.m@ims.operador.com
From: sip:eva.m@ims.operador.com;tag=sdfasfd
Call-ID: 2342sdfasdf
CSeq: 1 REGISTER
Via: SIP/2.0/UDP pcscfa_IP_address:port;branch=abc
Via: SIP/2.0/UDP UEC_IP_address:port;branch=xyz
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD;utran-cell-id="C359A3913B20E"
P-Charging-Vector: icid-value=5ecd46f
Contact: <sip:UEC_IP_address:port>;expires=3600
Route: <sip:icscfa_ip_addr:port;transport=udp;lr>
Content-Length: 0
```

Figura 28. Mensaje SIP tras incluir información sobre el P-CSCF correspondiente

El siguiente paso es localizar el S-CSCF. Para ello el I-CSCF envía una UAR Diameter al HSS, donde le transfiere la identidad pública de usuario y la privada de usuario y el identificador de la red, tomados desde la petición de registro SIP. El HSS autoriza al usuario en la red y valida que la Identidad Privada del Usuario está vinculada a esa Identidad Pública de Usuario

```
<RAR>  ::= < Diameter Header: 258, REQ, PXY >
           < Session-Id >
           { Origin-Host }
           { Origin-Realm }
           { Destination-Realm }
           { Destination-Host }
           { Auth-Application-Id }
           { Re-Auth-Request-Type }
           [ User-Name ]
           [ Origin-State-Id ]
         * [ Proxy-Info ]
         * [ Route-Record ]
         * [ AVP ]
```

Figura 29. Mensaje UAR con el nodo HSS durante la fase de registro

El HSS envía una UAR al I-CSCF, incluyendo una lista de S-CSCF con sus respectivas capacidades y prestaciones para asignar el más adecuado al usuario que va a registrarse.

El nodo I-CSCF dispone de una tabla configurable de los S-CSCF que operan en la red propia y las capacidades de cada uno de ellos según la información que proporciona el HSS, con lo que envía una petición SIP REGISTER al S-CSCF que haya sido seleccionado. Todas las peticiones REGISTER se autentican en la red IMS, sin embargo, las peticiones INVITE nunca siguen este proceso.

```
REGISTER sip:ims.Operator-X.com SIP/2.0
To: sip:eva.m@ims.operador.com
From: sip:eva.m@ims.operador.com;tag=edfaefd
Call-ID: 2342sdfasdf
CSeq: 1 REGISTER
Via: SIP/2.0/UDP icscfa_IP_address:port;branch=efg
Via: SIP/2.0/UDP pcscfa_IP_address:port;branch=abc
Via: SIP/2.0/UDP UEC_IP_address:port;branch=xyz
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD;utran-cell-id="C359A3913B20E"
P-Charging-Vector: icid-value=5ecd46f
Contact: <sip:UEC_IP_address_port>;expires=3600
Route: <sip:scscfa_ip_addr:port;transport=udp;lr>
Content-Length: 0
```

Figura 30 Mensaje SIP tras reencaminarlo el ICSCF

Ahora el S-CSCF contacta con el HSS con un doble propósito: por un lado necesita los datos de autenticación para el usuario en particular , y además necesita guardar su propia URI en el HSS. De este modo, en las futuras ocasiones en las que se vuelva a preguntar por el mismo usuario, se devolverá la dirección de éste S-CSCF. En este tipo de mensaje DIAMETER se encuentran campos como los que aparecen a continuación:

```
< Multimedia-Auth-Request > ::=  < Diameter Header: 303, REQ, PXY,
16777216 >
< Session-Id >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
[ Destination-Host ]
{ User-Name }
*[ Supported-Features ]
{ Public-Identity }
[ SIP-Auth-Data-Item ]
[ SIP-Number-Auth-Items ]
{ Server-Name }
*[ AVP ]
*[ Proxy-Info ]
*[ Route-Record ]
```

Figura 31. Mensaje Diameter en fase de registro desde el S-CSCF al HSS

A este mensaje, el HSS responde con una MAA que contiene las credenciales para la validación del usuario. Con esta información, el S-CSCF envía un mensaje LUR al HSS, con lo que consigue almacenar la URI en la base de datos. En la siguiente tabla se muestran los campos que contienen los mensajes DIAMETER:

Tabla 9. Campos del mensaje DIAMETER en fase de registro entre S-SCSF y el HSS

Campo	Descripción
Session-Id	Este campo identifica la sesión (authentication request) entre el cliente y el servidor Cx
Vendor Specific Application Id	Indica el 'vendor' (3GPP) al que pertenece la aplicación y el tipo de aplicación (authentication).
Origin-Host	Indica el punto donde se originó el mensaje Diameter.Suele contener la dirección del cliente Diameter
Origin-Realm	Contiene la dirección Realm del creador del mensaje Diameter..
Destination-Host	Indica la dirección del terminal final, o host destino. Contiene la dirección Cx del servidor Diameter.
Destination-Realm	Contiene la dirección Realm del servidor Cx destino.
Public User Identity	Identidad Pública de usuario o Identidad Pública de Servicio
S-CSCF Name	Nombre del S-CSCFs que se va a asignar Contiene dos parámetros: • Nombre de S-CSCF origen • Nombre de S-CSCF destino
Indication	Tipo de actualización que el S-CSCF solicita al HSS: • SET_S-CSCF_NAME • CLEAR_S-CSCF_NAME • UNREGISTERED_USER

Para indicar que se ha procesado satisfactoriamente el mensaje LUR, el HSS envía un mensaje LUA (Location-Update-Answer) al S-CSCF. Además, en este mensaje, se indica en el campo

Tabla 10. Campos del mensaje LUR/LUA del HSS

Campo	Mapeado a Diameter AVP	Descripción
Indication	Indication	Este elemento indica los cambios en el

Campo	Mapeado a Diameter AVP	Descripción
		perfil del usuario. Los posibles valores son: USER_PROFILE_CHANGED USER_PROFILE_NOT_CHANGED

A continuación, el S-CSCF envía un mensaje UDR (User-Data-Request) al HSS para obtener el perfil de usuario.

Tabla 11. Campos representativos del mensaje UDR

Campo	Mapeado a Diameter AVP	Cat.	Descripción
Auth Session State	Auth-Session-State	M	Indica si el estado se mantiene para una sesión particular.
Public User Identity	Public-Identity	M	Identidad Pública de Usuario o del servicio
Wildcarded PSI	Wildcarded-PSI	O	Identidad pública

El siguiente paso es que el HSS envíe una respuesta UDA con la información del perfil del usuario al S-CSCF. El contenido del mensaje es el mismo que el mostrado hasta ahora para el protocolo diameter, siendo relevantes:

Tabla 12. Campos representativos para el mensaje UDA

Campo	Mapeado a Diameter AVP	Cat.	Description
Public User Identity	Public-Identity	M	Identidad Pública de usuario o del servicio
Wildcarded PSI	Wildcarded-PSI	O	Wildcarded PSI correspondiente a la Identidad Pública.

Una vez recibida esta información desde el HSS, el S-CSCF procede a enviar al I-CSCF un mensaje SIP 200 OK, indicando que se ha realizado con éxito el registro del usuario.

```
200 OK SIP/2.0
To: sip:eva.m@ims.operador.com
From: sip:eva.m@ims.operador.com;tag=sdfasfd
Call-ID: 2342sdfasdf
CSeq: 1 REGISTER
Via: SIP/2.0/UDP icscfa_IP_address:port;branch=efg
Via: SIP/2.0/UDP pcscfa_IP_address:port;branch=abc
Via: SIP/2.0/UDP UEC_IP_address:port;branch=xyz
Contact: <sip:UEC_IP_address:port>;expires=3600
Content-Length: 0
```

Figura 32. Mensaje SIP 200 OK

A continuación el I-CSCF lo envía al P-CSCF correspondiente. Puede apreciarse la variación en los campos <via> del mensaje SIP:

```
200 OK SIP/2.0
To: sip:eva.m@ims.operador.com
From: sip:eva.m@ims.operador.com;tag=sdfasfd
Call-ID: 2342sdfasdf
CSeq: 1 REGISTER
Via: SIP/2.0/UDP pcscfa_IP_address:port;branch=abc
Via: SIP/2.0/UDP UEC_IP_address:port;branch=xyz
P-Access-Network-Info: 3GPP-UTRAN-TDD;utran-cell-id="C359A3913B20E"
Contact: <sip:UEC_IP_address:port>;expires=3600
Content-Length: 0
```

Figura 33.Mensaje SIP 200 OK (2)

Y Finalmente el P-CSCF recibe el mensaje 200 OK Register, y lo envía al usuario para notificar el correcto registro.

```
200 OK SIP/2.0
To: sip:eva.m@ims.operador.com
From: sip:eva.m@ims.operador.com;tag=sdfasfd
Call-ID: 2342sdfasdf
CSeq: 1 REGISTER
Via: SIP/2.0/UDP UEC_IP_address:port;branch=xyz
Contact: <sip:UEC_IP_address:port>;expires=3600
Content-Length: 0
```

Figura 34 Mensaje SIP 200 OK de notificación de registro

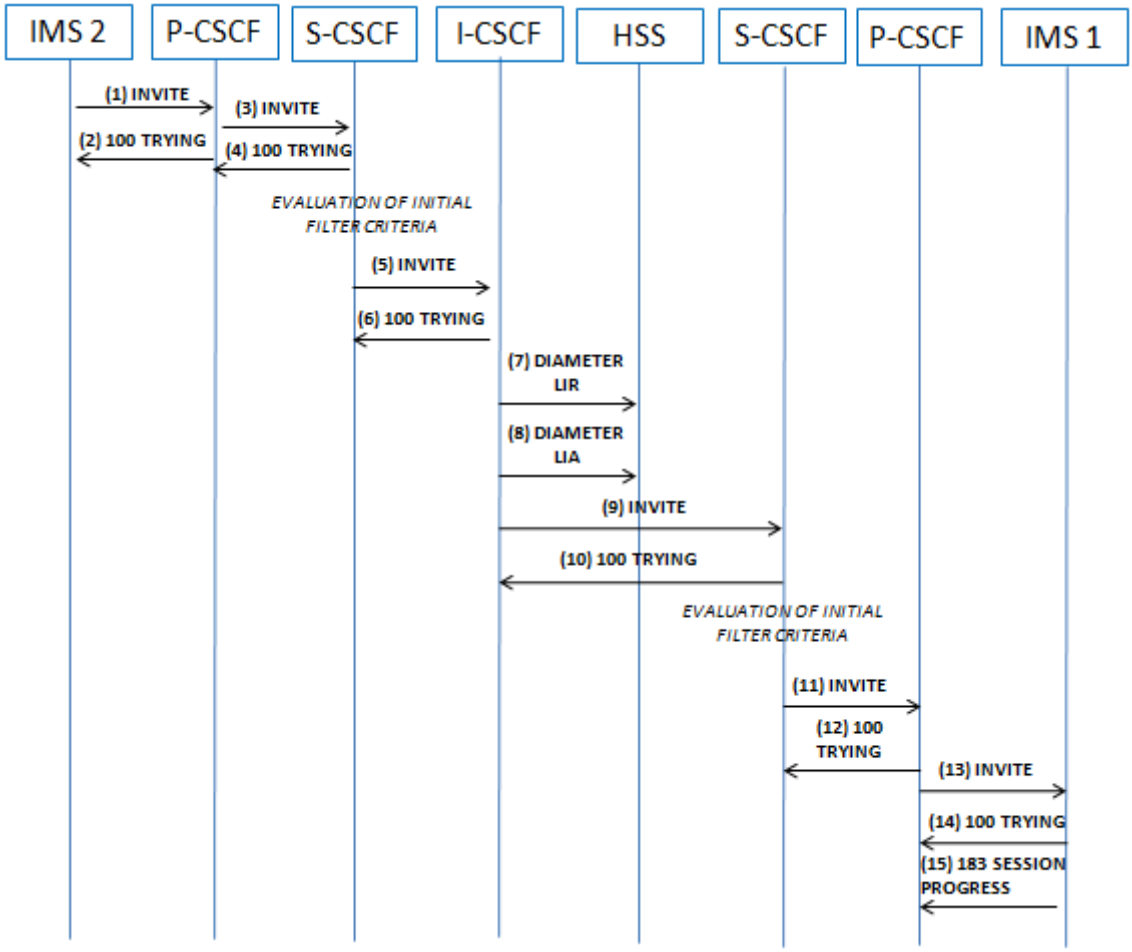
6.2. Llamada entre usuarios IMS

Una vez se ha completado el registro del usuario en la red, se procede a establecer una sesión. El concepto de sesión comprende las acciones que se realizan entre desde que se establece un intercambio de datos entre dos usuarios y el momento en el que cesa el intercambio. Supondremos el caso en el que un usuario A desee realizar una llamada de voz a otro usuario B de la red, es necesario establecer una sesión para intercambiar datos de voz sobre RTP.

En este apartado exploraremos el proceso de establecimiento de sesión básica en IMS, pero supondremos que tanto el terminal que establece la sesión como el que recibe la petición de establecimiento son terminales IMS y que soportan el mismo tipo de capacidades en la red. También, nos pondremos en la situación en la que ambos terminales hacen uso del servicio 'roaming', estando fuera de su red origen, 'Home Network'.

En la siguiente figura se aprecia la señalización requerida en el establecimiento de una sesión. Cuando hablamos de nodos originantes (Originating Network) nos referimos a los que dan servicio al terminal que origina la petición de sesión. De igual manera, cuando se hace referencia a los nodos de la red del terminal al que va destinada la petición (Terminating Network).

Una vez que se ha realizado con éxito el establecimiento de sesión, es posible comenzar con el intercambio de datos, hasta que uno de ellos decida finalizar, momento en el que tratándose de tráfico de voz, finaliza la sesión.



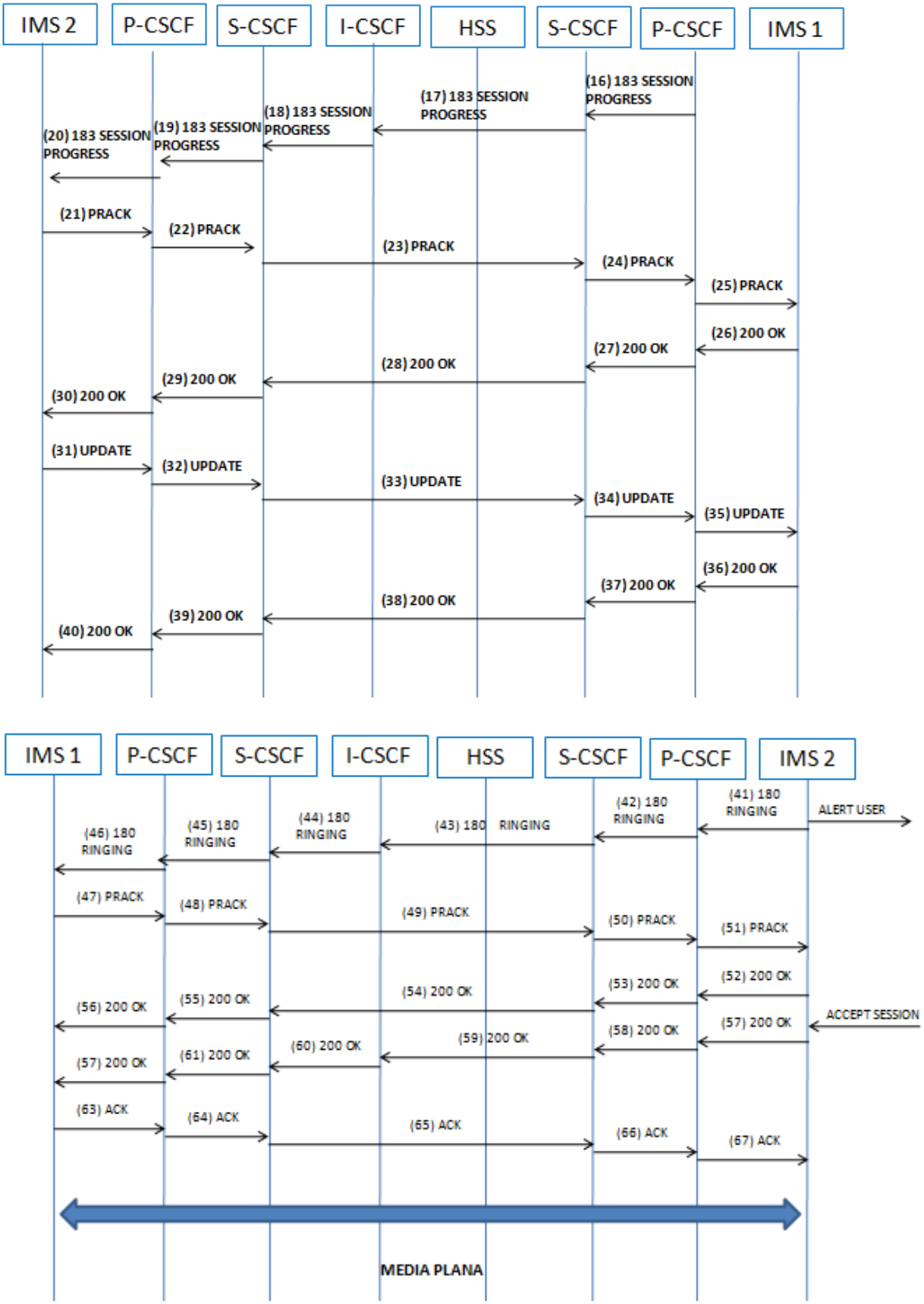


Figura 35. Flujo de la llamada entre dos usuarios IMS

En la siguiente tabla numeramos la secuencia de mensajes que se originan en este proceso.

Tabla 13. Flujo de la llamada entre usuarios IMS

Número de mensaje	Descripción
1	El usuario UE, envía un mensaje INVITE SIP al P-CSCF.
2	El P-CSCF contesta al usuario con un mensaje SIP 100 TRYING También reemplaza el campo <P-Preferred-Identity> por <P-Asserted-Identity> que contiene el mismo valor de Identidad de Usuario
3	Una vez contestado 100 TRYING al usuario, reenvía la petición INVITE al S-CSCF
4	EL S-CSCF devuelve 100 TRYING al P-CSCF
5	EVALUATION CRITERIA S-CSCF reenvía de nuevo el mensaje INVITE hacia el I-CSCF
6	I-CSCF contesta al S-CSCF con 100 TRYING
7	EL I-CSCF envía un mensaje DIAMETER, LIR () al HSS
8	El HSS contesta mediante DIAMETER un mensaje LIA () al I-CSCF
9	A continuación el I-CSCF envía la petición ENVITE al S-CSCF (terminating network)
10	S-CSCF contesta SIP 100 TRYING
11	EVALUATION OF INITIAL CRITERIA: El S-CSCF envía la petición INVITE al P-CSCF del usuario final (terminating visited network)
12	P-CSCF contesta con SIP 100 TRYING
13	P-CSCF envía la petición SIP INVITE al terminal IMS final
14	El terminal IMS devuelve 100 TRYING al P-CSCF y alerta al

	usuario
15-20	El terminal notifica con un mensaje SIP 183 SESSION PROGRESS al P-CSCF(Terminating Visited Network) y se va reenviando al S-CSCF(Terminating Home Network), I-CSCF (Terminating Home Network), S-CSCF (Originating Home Network) , P-CSCF(Originating Visited Network),hasta que llega al terminal que originó la petición.
21-25	El terminal procede a enviar un mensaje SIP PRACK al P-CSCF(Terminating Visited Network), que se reenvía al S-CSCF(Terminating Visited Network), S-CSCF (Terminating Home Network) , P-CSCF (Terminating Visited network) hasta llegar al terminal final IMS
26-30	El terminal final IMS notifica con un mensaje SIP 200 OK la petición PRACK. Este mensaje pasa por los nodos P-CSCF(Terminating Visiting Network) , S-CSCF (Terminating Home Network), I-CSCF(Terminating Home Network), S-CSCF (Originating Home Network) , P-CSCF(Originating Visited Network),hasta que llega al terminal que originó la petición.
31-35	El terminal procede a enviar un mensaje UPDATE al P-CSCF(Terminating Visited Network), que se reenvía al S-CSCF(Terminating Visited Network), S-CSCF (Terminating Home Network) , P-CSCF (Terminating Visited network) hasta llegar al terminal final IMS
36-40	El terminal final IMS notifica con un mensaje SIP 200 OK la petición anterior pasando por los nodos P-CSCF(Terminating Visiting Network) , S-CSCF (Terminating Home Network), S-CSCF (Originating Home Network) , P-CSCF(Originating Visited Network),hasta que llega al terminal que originó la petición.
41-46	El terminal final IMS alerta al usuario de la petición y genera el mensaje SIP 180 RINGING, pasando por los nodos P-CSCF(Terminating Visiting Network) , S-CSCF (Terminating Home Network), I-CSCF(Terminating Home Network), S-CSCF (Originating Home Network) , P-CSCF(Originating Visited Network),hasta que llega al terminal que originó la petición.

47-51	El terminal origen procede a enviar un mensaje PRACK al P-CSCF(Terminating Visited Network), que se reenvía al S-CSCF(Terminating Visited Network), S-CSCF (Terminating Home Network) , P-CSCF (Terminating Visited network) hasta llegar al terminal final IMS
52-56	El terminal final IMS notifica con un mensaje SIP 200 OK la petición anterior pasando por los nodos P-CSCF(Terminating Visiting Network) , S-CSCF (Terminating Home Network), S-CSCF (Originating Home Network) , P-CSCF(Originating Visited Network),hasta que llega al terminal origen.
57-62	EL terminal final IMS acepta la sesión, y por consiguiente genera un mensaje SIP 200 OK que se reenvía por los nodos P-CSCF(Terminating Visiting Network) , S-CSCF (Terminating Home Network), I-CSCF (Terminating Home Network), S-CSCF (Originating Home Network) , P-CSCF(Originating Visited Network),hasta que llega al terminal que origen
63-67	El terminal origen procede a enviar un mensaje de aceptación ACK al P-CSCF(Terminating Visited Network), que se reenvía al S-CSCF(Terminating Visited Network), S-CSCF (Terminating Home Network) , P-CSCF (Terminating Visited network) hasta llegar al terminal final IMS
68	En este momento,una vez completado el establecimiento de la sesión se procede al intercambio de datos en el plano de media.

Como se aprecia, toda la señalización se encamina a través del P-CSCF y el S-CSCF (tanto del terminal origen como del destino) Cada uno de estos nodos inserta en la cabecera de los mensajes un ‘Record route’ que almacena su propia SIP URI, garantizando que los posteriores mensajes de señalización atraviesen dichos nodos, como por ejemplo ‘PRACK’, ‘200 OK’, ‘BYE’, etc. EN el I-CSCF la situación cambia, ya que sólo atraviesan el nodo las peticiones ‘INVITE’ y sus respectivas respuestas, por tanto sólo introduce el campo en la cabecera de estas peticiones.

También es muy importante notar, que la interacción DIAMETER se lleva a cabo entre el I-CSCF y el HSS en la ‘Home Network’ del terminal destino, ya que es necesario conocer el S-CSCF asociado a este usuario.

Hasta ahora todo lo analizado hace referencia a la señalización, pero hablemos del control de los nodos. EL AS, será el encargado de gestionar toda la lógica. Dentro de

la red IMS, generalmente existen varios AS, cada uno especializado en servicios distintos, y con una arquitectura diferente, pero todos permiten el protocolo SIP en el interfaz con el S.CSCF, conocido como ISC (IMS Service Control Interface). EL AS puede localizarse en la 'Home Network' o en otra distinta, pero es criterio del S-CSCF involucrar al AS en el proceso de establecimiento de sesión.
A continuación se presentan de manera sintetizada ejemplos de tráfico en la red, ya que la señalización llevada a cabo es similar a la ya expuesta.

6.3. Llamada entre usuario de la red fija y usuario de la red IMS

Si tenemos el caso en el que un usuario de la red fija desea establecer una sesión con otro usuario de la red IMS, los datos tendrán que pasar por el nodo MGCF que es el punto de entrada a la red IMS desde la red de conmutación.

El usuario enviará su identificación, y en este caso corresponde al número de teléfono. Dentro de la red IMS, es necesario disponer de una SIP URI para poder realizar la señalización, por lo que el MGCF se comunica con el DNS/ENUM para obtener la Identidad Pública del usuario de la red fija. Una vez recibida la información se reenviará hacia el I-CSCF en un mensaje INVITE. Desde este punto, la señalización será exactamente igual que si la llamada se realizara entre usuarios de la misma red IMS siendo el MGCF el nodo que adapta las respuestas hacia la red conmutada. La adaptación del tráfico se lleva a cabo en el nodo IMS-MGW.

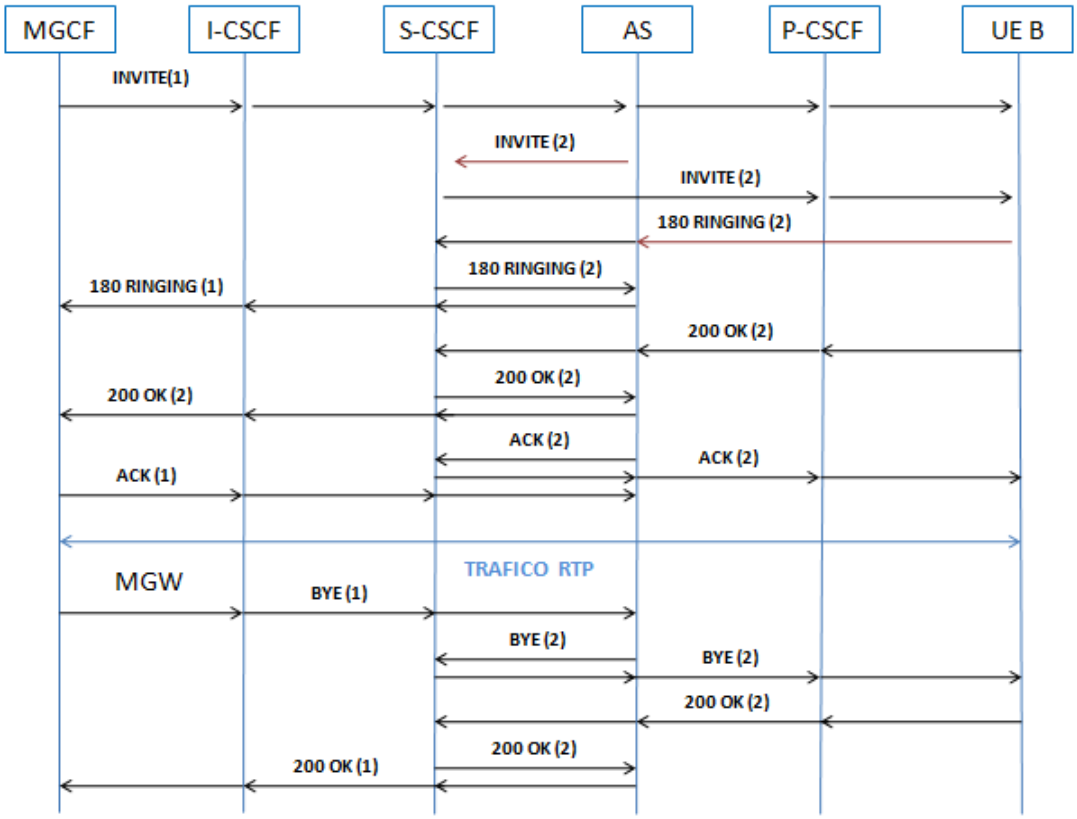


Figura 36. Llamada entre un usuario IMS y usuario de la red fija.

Los indicativos (1) y (2) de la figura hacen referencia al UA1 o UA2

6.4. Llamada de un usuario IMS a un usuario de la red fija

Si suponemos que un usuario de la red IMS quiere establecer sesión con uno de la red fija, debe enviar su Tel URL con el número de teléfono del usuario final e incluirlo en la 'Request-URI' del mensaje SIP INVITE. Este mensaje INVITE se envía al P-CSCF correspondiente y a su vez se reenvía al S-CSCF. Desde este nodo, hay que hacer la consulta al DNS/ENUM para obtener el número de teléfono del terminal destino a partir de la Tel URL. Al tratarse de un usuario no IMS, el DNS no es capaz de devolverle al S-CSCF dicha información, tomando otra alternativa.

El siguiente paso es contactar desde el S-CSCF con el BGCF. El BGCF dispone de una base de datos donde averigua que el número de teléfono solicitado pertenece a la red fija y encamina la petición hacia el MGCF.

En el nodo MGCF se realiza la conversión de SIP a ISUP para enviarla a la red fija. Para el intercambio de voz, vuelve a ser el IMS-MGW el punto de enlace entre ambas redes.

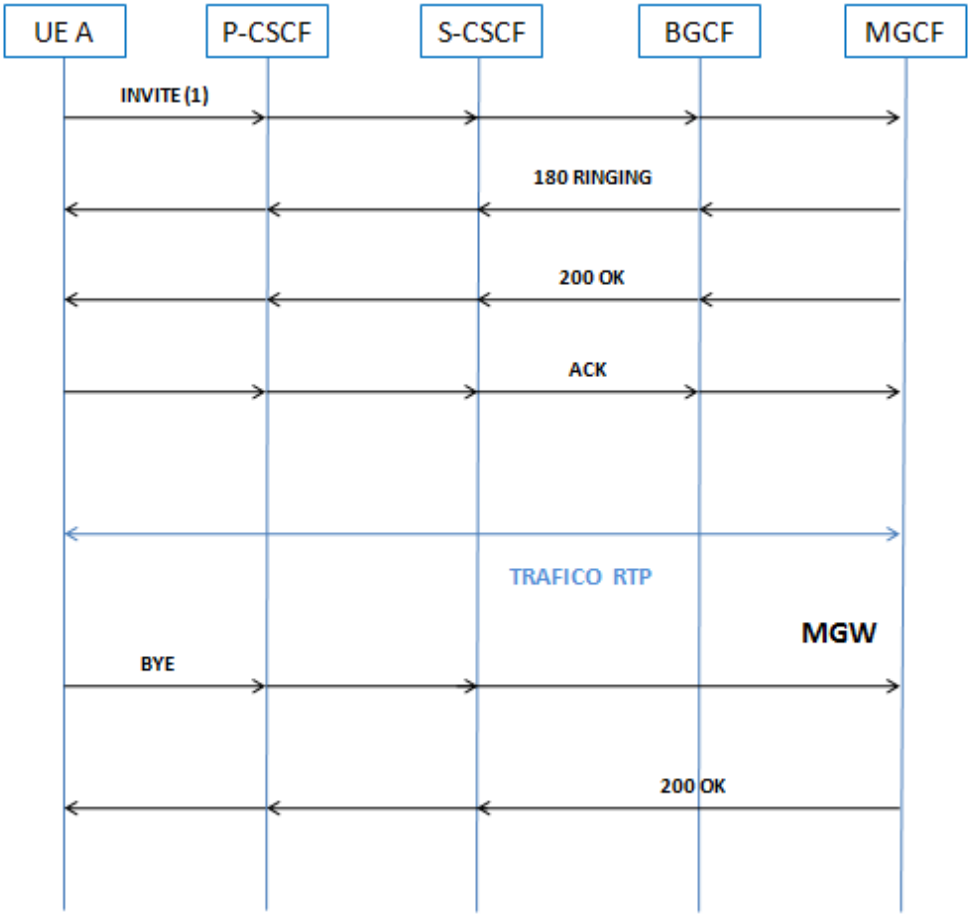


Figura 37. Llamada desde un usuario IMS a un usuario de la red fija

7. Caso práctico

En este capítulo se expone un caso práctico de diseño para una implementación IMS en una red comercial. Se trata de ampliar la capacidad de la red existente mediante la incorporación de nuevo elementos en la red o el reemplazo de los existentes.

7.1. Descripción del servicio

El servicio conocido como 'Business Trunking' conecta centralitas de conmutación (PBX) a la dirección IP pública de la red IMS del operador, al tiempo que proporciona los medios para identificar si el tráfico es de datos o de voz.

EL servicio permite ahorros OPEX en la infraestructura IP, permitiendo voz y datos en la misma conexión. Realiza una serie de tareas valiosas para asegurar la conexión de las empresas que lo comparten. Valida las llamadas PBX origen y facilita el control de la facturación.

Está orientado a empresas que dispongan de centralitas PABX ya sean SIP o H.323 que cursen tráfico interno entre distintas sedes del cliente.

La red del operador soporta SIP y el interfuncionamiento con H.323. A su vez, los clientes tendrán que disponer de equipos capaces de manejar servicios de telefonía sobre IP (centralitas IP, servidores de llamadas…) y que utilicen portocolo SIP o H.323

7.2. Objetivo

El objetivo del proyecto es la inclusión de un nuevo cluster de SBC en la red IMS de un operador. El equipo SBC será un '*hardware*' con una capacidad 3,5 veces mayor que el resto de SBCs que dispone en la red, con vistas a atender la demanda creciente de usuarios del próximo año. Generalmente el despliegue de 'clusters' de SBC's se realiza por parejas, debido a que se reparte el tráfico al 50% entre dos cluster para que, si se diera el caso en el que un nodo fallara, el otro sea capaz de asumir todo el tráfico.

Para el servicio de interconexión de empresas '*Businnes Trunking*' (BT), los nuevos SBC podrán comunicarse con los AS que ya existen en la red y que proporcionan / gestionan este servicio.

7.3. Diagrama de red

La red existente del operador cuenta con la siguiente estructura:

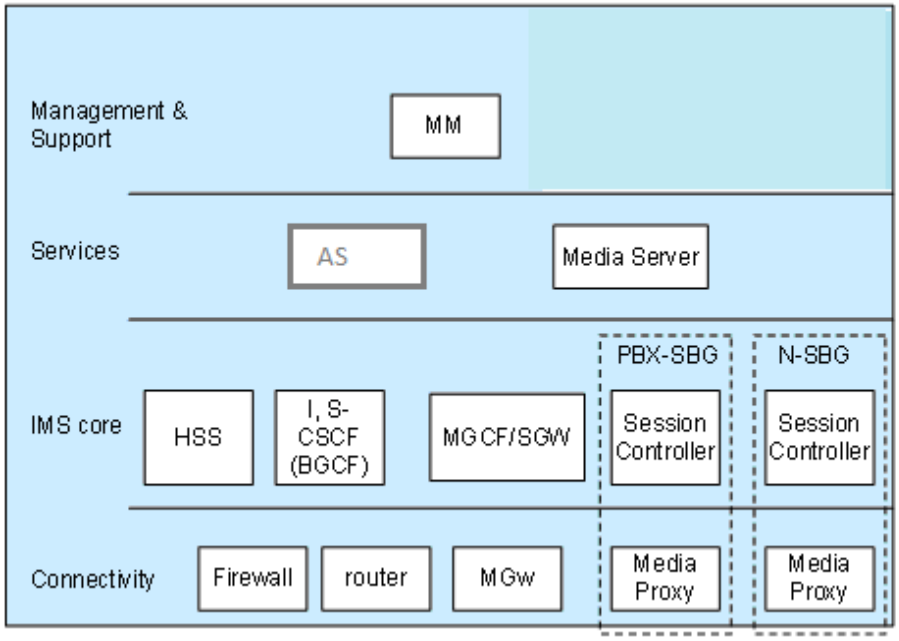


Figura 38. Estructura de solución de área de negocio para grandes clientes.

Desde el punto de vista de los nuevos nodos que se van a instalar, tendríamos un esquema:

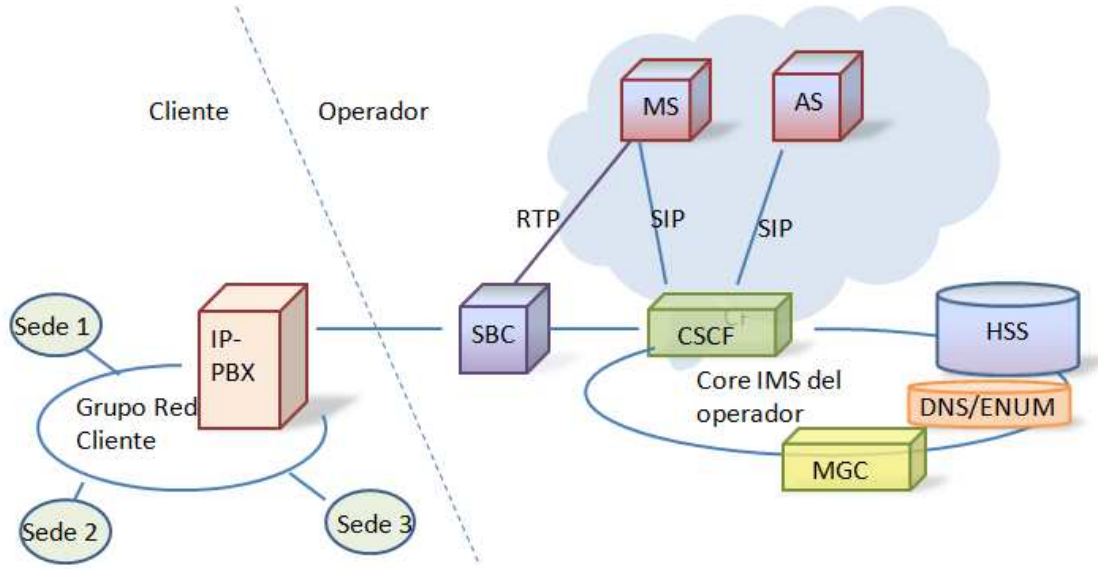


Figura 39. Esquema de red para la conexión BT

Integramos por tanto la red con los siguientes principales elementos:

- CSCF:

  En la planta del operador hay desplegados dos nodos CSCF (redundancia con balance de carga al 50%).

  El CSCF recibirá peticiones INVITE SIP que le envíe el SBC. Una vez realizada la acción se comunicará con el DNS para la búsqueda del AS destino correspondiente.

- HSS:

  En la red también se dispone de dos nodos HSS redundados trabajando uno como 'hot' y el otro como 'stand-by'. En la base de datos de los HSS se define únicamente el perfil del AS que da servicio a los grandes clientes. En el AS es donde reside toda la lógica del servicio Interconexión grandes clientes, por tanto cuando el CSCF consulte con el HSS si una llamada entrante a la red desde la centralita de grandes empresas puede o no acceder al servicio, tendrá que encontrar la dirección del AS solicitado mediante consulta al DNS.

- SBC

  El nodo SBC como ya hemos mencionado anteriormente, se desplegará siempre emparejado como un '*cluster*' para garantizar redundancia. En un nodo que

permite el acceso a la red IMS a los usuarios (puede configurarse con funcionalidad de P-CSCF, como punto de entrada a la red).
Proporciona por tanto el acceso a red a los usuarios, y resuelve sus necesidades de conectividad, direccionamiento y enrutamiento.
Mediante el servicio BT, no se registran los usuarios en la red, solamente la centralita establece una realción para poder utilizar el núcleo de red. Por este motivo el SBC también se encargará de aportar al núcleo de red la información que necesite sobre un acceso concreto.
La relación que se establece entre el SBC y las IP-PABX
Únicamente la PABX-IP establece dicha relación para utilizar este Núcleo de Red IMS en modo tránsito.

- El SBC posee interfaces virtuales que prestan conectividad a una empresa dentro de las interfaz física
- Estas interfaces lógicas llevan asociado un direccionamiento dentro de la VPN de la Empresa
- Cada una de las IP-PABX, tendrá asignado su direccionamiento IP, dentro de la VPN de la empresa.

- MGC / MGW

Se encuentran desplegados dos MGW, asociado cada uno a un MGC diferente.
Si se establecen llamadas desde la RTC hacia la red IMS el MGC tendría que obtener el dominio que hay que emplear en la 'Request-URI' de SIP INVITE. El resultado es la dirección del I-CSCF tras consultar DNS / ENUM.

- DNS/ENUM

El DNS/ENUM realiza la traslación de las Tel URL a las SIP URI. Gestiona la BBDD en disco donde se provisionan nuevos datos y su sincronización con las BBDD locales.

Se definen las SIP URI con la forma Prefix1@operador.ims.net para el servicio IGC . También se carga en el HSS estando este perfil definido en el HSS asociado a un 'trigger' que contiene la información de los AS a los que debe disparar.

- AS

Los AS soportan interfaces que permiten que se obtengan y actualicen campos de una BBDD para los servicios ofertados y enviar datos de tarificación al nodo que maneje el sistema de facturación.

Se encargan de validar al número de llamada entrante y la facturación podrá realizarse según el modelo que se haya establecido.

Generalmente, para el servicio de interconexión para grandes clientes los AS realizan las siguientes acciones:

-Definición de Llamada. Se definen los tipos de tráfico y se asigna un prefijo de operador en función del tipo al que pertenezca.

-Se establecen prefijos de encaminamiento para asignar a cada tipo de llamada un prefijo distinto (utilidad para la gestión de grupos)

- Restricción de llamadas: es posible restringir las llamadas, según los tipos de llamada asignados a un grupo o a un usuario.

- Control de Sesiones Simultáneas: se permite controlar el máximo de sesiones simultáneas establecidas (independientemente de que sean entrantes o salientes).

- Locuciones: gestiona los mensajes de error que se puedan ocasionar por motivo de congestión, indisponibilidad de servicio, etc. Los errores se tratan mediante mensajes SIP, y se contaría con la intervención del MS en estos casos.

- Redundancia de SBC: en el AS se configura un FQDN con el fin de que el CSCF pueda enrutar el tráfico a los cluster de SBC's en reparto de carga tras consultar al DNS.

- MS

Los nodos MS desplegados en la red generan los mensajes de error. Las causas de error se reciben mediante mensajería SIP y el correspondiente mensaje de error

asociado a cada mensaje se configura directamente en el MS. Las locuciones las pueden descargar de un AS.

7.4. Especificación de distintos grupos dentro de la empresa

El cliente ha solicitado ciertos servicios IMS para todos los usuarios de la empresa, la cual tiene un servicio de Red Privada Virtual con el operador (MLAN/ VPN /IP) para comunicar sus sedes internamente. A la hora de gestionar el tráfico y las funcionalidades desde los nodos IMS, se definen los siguientes grupos:

Grupo: formado por un conjunto de sedes cuyas llamadas se gestionan en la misma IP-PBX del cliente.
Sede: usuarios con la misma ubicación física o lógica con la misma numeración pública para el establecimiento de llamadas externas.
Usuario: Cada número público que forma una sede.

Por tanto, el conjunto empresa se divide en grupos y éstos a su vez en sedes, que son conjuntos de usuarios. Para la gestión de las llamadas, se definen además los siguientes prefijos para las llamadas salientes o entrantes:

- OPrefix1: Prefijo que permite enrutar una llamada saliente de una centralita IP-PBX , hacia una pareja de AS. Tendría el formato oprefix1@operador.ims.net.
- IPrefix1: Prefijo que permite enrutar una llamada entrante a una centralita IP-PBX , a la pareja de AS. Presentaría la forma Iprefix1@operador.ims.net.

7.5. Parámetros de referencia

Dentro de los mensajes y peticiones SIP que se generarán durante el flujo de las llamadas, caben destacar los siguientes como básicos a la hora de enrutar el tráfico:

- ‘Request URI’: indica el usuario al que va dirigida la petición.
- ‘To’: suele coincidir con la Request-URI

Dentro del mensaje encontramos la siguiente información:

  - o <Trunk Context>: Identificción de la empresa destino (VPN)
  - o <Tgrp>: Identificación de la IP-PABX destino.

- 'Route': dirección IP para alcanzar cierto destino.
- 'Contact': indentifica al usuario que crea la petición. Suele tomar el mismo valor que 'From'. Dentro del campo encontramos:

  - o <Trunk Context>: Identifica la empresa origen (VPN)
  - o <Tgrp>: Identifica a la IP-PABX origen
  - o <P_Assert_I>D: número llamante

7.6. Impacto en red IMS con la inclusión de un nuevo cluster de SBC

Si a la red existente del operador le añadimos las dos parejas de SBC necesarias para la ampliación de la capacidad del servicio de interconexión a grandes clientes, se verían afectados otros nodos del Core en los que habrá que enrutar y configurar una serie de parámetros.

El SBC en esta implementación, se configura con funcionalidad P-CSCF. Como consecuencia de ello, el primer nodo de la red en el que hay que configurar una serie de parámetros es en el CSCF. También necesitaremos incluir datos nuevos en el DNS y configuraciones en el MGC.

- CSCF: Se crea una nueva entrada con la normalización del número

```
NumNormSubstitutionEntry:servicio.operador.ims.net
```

- DNS / ENUM: se añaden los registros RPV/A de los AS y los MS del servicio en cuestión al que va a dar soporte el cluster de SBC.
- MGC:

- Se añade un nuevo 'routing case' de SIP para que el MGC pueda realizar consultas ENUM:
  <Use_ENUM_type_routing> = TRUE
- Se crea un nuevo 'profile' que permita al nodo enviar la Request-URI en formato Tel-URI hacia el CSCF.
- Por último se actualiza la tabla de análisis 'B-Number': al definir el parámetro <sipProfileUriScheme=Te>, el formato del Request-URI que se envia al I-CSCF es Tel-URI.

- HSS: en el HSS hay que definir los usuarios genéricos que van a utilizar el servicio, IPrefix1 y OPrefix2. A continuación se muestra un ejemplo de perfil para uno de los usuarios.

IPrefix1:

```
HSS-SubscriberID: IPrefix1@servicio.operador.ims.net
HSS-SubscriberBarringInd: FALSE

HSS-PrivateUserID: IPrefix1@servicio.operador.ims.net
HSS-AllowedAuthMechanism: Digest
HSS-ChargingProfId: DefaultChargingProfile
HSS-IsPsi: FALSE
HSS-MaxCallLegs: 64000
HSS-MaxSessions: 64000
HSS-PrivacyIndicator: FALSE
HSS-RoamingAllowed: TRUE
HSS-SipLocked: FALSE
HSS-UserBarringInd: FALSE

HSS-PublicIdValue: sip:IPrefix1@servicio.operador.ims.net

HSS-ImplicitRegSet: 1
HSS-IsDefault: TRUE
HSS-PublicIdValue: sip: IPrefix1@servicio.operador.ims.net
HSS-SessionBarringInd: FALSE
HSS-UserServiceProfileId: IPrefix1@servicio.operador.ims.net
HSS-XcapAllowed: FALSE

HSS-PublicIdValue: tel:+34913060840
HSS-ImplicitRegSet: 1
HSS-IsDefault: TRUE
HSS-SessionBarringInd: FALSE
HSS-UserServiceProfileId: IPrefix1@servicio.operador.ims.net
```

Figura 38. Ejemplo de perfil cargado en el HSS

- SBC: para cada pareja de SBC se definen los interfaces:
  -IP, máscara y submáscara de red para el interfaz de Gestión.
  -IP y VLAN para el Acceso público a la red. También su máscara de red.
  -IP y VLAN para el flujo RTP.

-IP y VLAN para señalización.

- Para el Core se definen dos NI (“*Network Interfaces*”) una de señalización-servicio y otra para flujo RTP. También se define una VLAN de redundancia por si existiera caída de uno de los router. (La redundancia suele estar basada en el ‘time-out’ del protocolo ARP, descubrimiento de la dirección MAC)

- El ‘SIP-interface’ define las direcciones de transporte (direcciones IP y puerto) sobre los que el SBC recibe y envia mensajes SIP:

sip-interface

state	enabled
realm-id	SIP.ICSCF.Servicio // en el Core
	SIP.SBC // en el SBC
sip-port address	192.168.1X.90 // En el core
	127.255.255.X // En el SBC
port	5060
transport-protocol	UDP
term-tgrp-mode	iptel *//Para detección de parámetros de trunk group.*

Figura 39. Definición de SIP Interface en el Core y el SBC.

Para el correcto funcionamiento del servicio, durante el flujo de llamada, el SBC tendrá que realizar modificaciones en las cabeceras de los mensajes de señalización. En la siguiente tabla se muestran las más significativas:

Tabla 14. Modificaciones que realiza el SBC en los mensajes SIP para tráfico entrante y saliente

Manipulaciones en SBC	**Manipulación entrante**				**Manipulación saliente**
Cabecera	**Request-URI**	**Contact**	**To**	**From**	**Request-URI**
Manipulación	Reemplazar contenido de uri-user por IPrefix1	Añadir parámetros tgrp *y* trunk-context	Copiar el contenido del R-URI. Añadir parámetro user=phone.	Añadir parámetro user=phone.	Borrar tgrp y trunk-context Envio la IP de la PBX en lugar del dominio.

7.7. Provisionamiento

Para este apartado sólo se considerará la provisión de IP-PBX's soportando el protocolo SIP.

Los siguientes elementos serán provisionados en el SBC. Si utilizamos una ruta adicional en una empresa, estos objetos se crearán una única vez. Si se utilizan las dos rutas alternativas se crearán dos veces y así sucesivamente.

- Network-Interface (NI): *Uno por empresa.*
- Realm: Identifica el contexto dentro del SBC de la empresa para el servicio que se oferta.. Se asocian al mismo Network-Interface.
- Sip-interface: Interfaz SIP hacia Realms
- Steering-pool: Dirección IP y rango de puertos UDP empleados para RTP. Válido para todas las PBX's de la empresa que se conecten a la ruta establecida.

Los siguientes objetos deben ser configurados por cada IP-PBX que se conecte a una ruta (tantos veces como conexión a rutas adicionales tenga):

- **Realm:** Identifica a la Sede en la cual se encuentra la IP-PBX y a la que se presta el servicio.

- **Session-Agent**: Identifica la IP-PBX. Define los campos que pueden manipularse, direccionamiento y protocolo utilizado.
- **Local-Policy**: Para permitir el acceso al Core (I-CSCF) es necesario permitir el acceso desde el 'realm hijo' a la PBX.

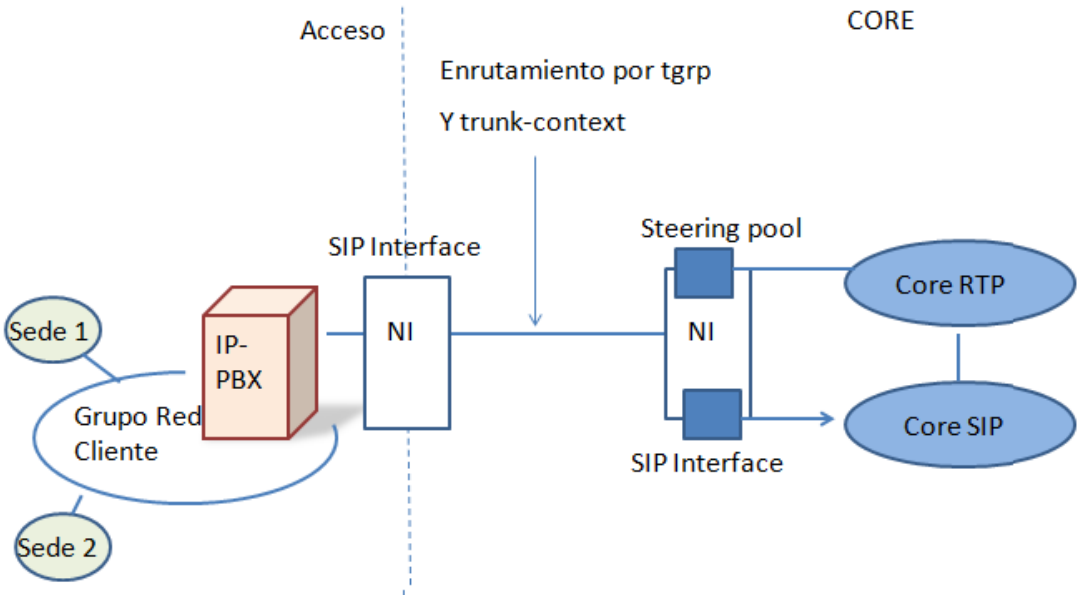


Figura 40. Esquema representativo de red con SIP Interface y Steering pool

-Para cada empresa un NI

-Para la PBX SIP de la empresa añadir:

- Un realm SIP (padre)
- Un SIP Interface (puerto SIP)
- Un Steering Pool

```
steering-pool
        ip-address          194.179.10.4    // Dirección IP de señalización del SIP-
interface SIP
        start-port          10000
        end-port            10999
        realm-id            sip_pbx // Indica el nombre del realm padre en este
caso el que correspondiente a la empresa.
        network-interface   XX
```

-Por cada PBX SIP añadir:

- Un realm (hijo)
- Un Session-Agent.

-Si la empresa dispone de PBX H323, por cada una de ellas añadir:

- Un realm
- Un H.323 Stack
- Un Steering Pool
- Un Session-agent

Algunos de los parámetros más representativos del Session-agent son:

```
session-agent
        hostname                    Sede1  // Indica el nombre de la PBX SIP de
una sede
        ip-address          10.81.X.X      // Dirección IP de la PBX
        port                5060
        state               enabled
        app-protocol                SIP
        transport-method            UDP
        realm-id            R.Sede1  // Nombre del realm de la PBX SIP
        allow-next-hop-lp           enabled
                max-sessions                        X
        max-inbound-sessions        X      // Permite configurar máximo número
de sesiones entrantes
        max-outbound-sessions       X      // Permite configurar máximo número
de sesiones salientes
```

Figura 41. Ejemplo de parámetros representativos del SIP-session-agent

Al igual que el resto de campos, el H.323 stack define parámetros de configuración para el enrutamiento con datos sobre direccionamiento, sesión…

En el propio SBC, se definen los siguientes parámetros:

Tabla 15. Parámetros de configuración para el 'provisioning' en el SBC

Campo	Ejemplo	Significado
name	SBC-Core	Nombre de Interfaz físico
sub-port-id	59	Identificador de VLAN.
ip-address	192.168.10.2	Dirección IP de interfaz.
pri-utility-address	192.168.11.2	Dirección IP MAC física empleada para el proceso de redundancia en el cluster
sec-utility-address	192.168.11.3	Dirección IP de MAC física empleada para proceso de redundancia en cluster en el sistema secundario
netmask	255.255.255.224	Máscara de subred
gateway	192.168.X.X	Puerta de enlace del sistema primario del cluster
retry-count	3	Número de reintentos de heartbeats antes de considerar el nodo "unreachable"
retry-timeout	3	Número de segundos que transcurren desde que el nodo cae e iniciar el siguiente heartbeat.

7.8. Llamadas desde el cliente hacia la red IMS del operador

Cuando se presenta el caso en el que una llamada sale desde la centralita IP-PABX del cliente hacia la red IMS del operador, las peticiones INVITE son enviadas desde la centralita IP-PABX hacia los SBC. Hay que notar, que el SBC se configuraría de tal modo que actúe como P-CSCF en la red.

Dentro del mensaje INVITE que llega al SBC, aparcería la siguiente información:

Campos ‘Request-UR’I y’ To’ con la información correspondiente del usuario receptor (UA1)

Campos ‘From’ y ‘Contact’ con la información del usuario emisor (UA2)

```
INVITE <sip:UA2@ims.Operator-X.com> SIP/2.0
Via: SIP/2.0/UDP UE_E_IP_Address:port;branch=abc
To: <sip: UA2@ims.Operator-X.com>
From: <sip:UA1@ims.Operator-X.com>
Call-ID: 1234567898-179612497@UE_E_IP_address
CSeq: 9057 INVITE
Contact: <sip:UE_E_IP_Address:port;transport=udp>
Allow:
INVITE,ACK,OPTIONS,BYE,CANCEL,INFO,REGISTER,PRACK,UPDATE,MESSAGE,REFER
,NOTIFY,PING
Max-Forwards: 69
Supported: preconditions,100rel, path,replaces,timer
P-Access-Network-Info: 3GPP-UTRAN-TDD;utran-cell-id="C359A3913B20E"
Session-Expires: 1800
Content-Length: xyz
....

v=0
o=- 50376 50376 IN IP4 UE_E_PORT_IP_Address
s=-
c=IN IP4 UE_E_PORT_IP_Address
t=0 0
m=audio 57938 RTP/AVP 107
a=rtpmap:107 AMBE-2/8000/1
a=fmtp:107


--boundary1


…

</ims-3gpp>

--boundary1--
```

Figura 43. Ejemplo de petición INVITE con parámetros representativos

Por otro lado, el SBC, realiza una modificación sobre el mensaje SIP INVITE que recibe. Debe enrutar el mensaje hacia los AS específicos del servicio e incluye la dirección del AS correspondiente en el campo Request-URI del mensaje.

Además es capaz de reconocer la IP-PABX que origina la llamada con la dirección física que recibe y el cliente, por el interfaz lógico por el cual se recibe la llamada (VPN). Al reconocer estos datos los incluye en la petición dentro del campo 'contact':
<trunkContext> : VPN A (RPV)
<Tgrp>: IP-PABX

```
INVITE <sip:AS.1@ims.Operator-X.com> SIP/2.0
...

To: <sip:UA2@ims.Operator-X.com>
From: <UA1@ims.Operator-X.com>
...

Contact: sip:UA1@ims.Operator-X.com

...
```

Figura 44. Ejemplo de petición INVITE con parámetros significativos (2)

Al actuar el SBC como P-CSCF, desde aquí se solicita descargar el perfil de usuario al HSS. Dispone del FQDN para consultar al DNS la dirección VIP de los AS a los que el CSCF debe enviar la petición.

Desde los AS se analiza el parámetro 'Request-URI' y comprueba que el parámetro que contiene 'From' pertenezca a la IP-PABX que se indica en el campo <Tgrp>, y a la empresa asociada a la VPN A que se indica en el campo <trunkContext> esté en la lista global de usuarios que dispone y lo reenvía al CSCF indicando si es o no correcta la identificación:

- Si la identificación es correcta, aparece:

  -Request-URI : UA2

  - Trunk Context=VPN B (RPV)
  - Tgrp = IP-PBX B

  -Route: FQDN que resolverá el CSCF tras consultar al DNS para obtener la IP del Cluster SBC del Servicio "IGC" donde ese encuentra registrado el Cliente destino al que va dirigida la llamada.

  -To: UA2

  -From: UA1

  -Contact: UA1

  - Trunk Context: VPN A (RPV)
  - Tgrp IP-PBX A

Y en el campo ‘Route’ el CSCF incluye la dirreción IP del cluster de SBC en el que está definido el cliente que generó la petición.

El CSCF recibe entonces la llamada con la nueva información en ‘Route’ y la reenvía de nuevo al SBC. Ahora el SBC es capaz de conocer la VPN del Cliente y la IP-PABX donde entregar el INVITE gracias a la información de <trunk context> y <Tgrp>.

- Si la identificación no es correcta, el CSCF toma el campo ‘Route’ como aparecía en el mensaje, y tendrá que consultar al DNS:
    - Si la consulta al DNS es satisfactoria, el UA2 pertenece a otro servicio soportado sobre la Red. Entonces se consulta al HSS para su localización.
    - Si la consulta al DNS no es satisfactoria, quiere decir que UA2 es un número externo a la red IMS del operador, por lo que CSCF reenviará el INVITE al MGC, para que se encamine hacia la RTB.

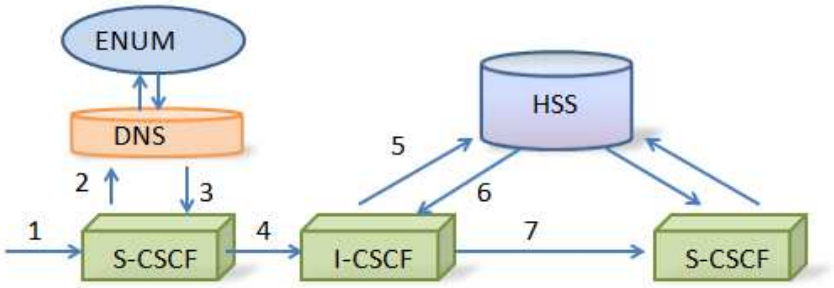


Figura 41. Verificación de la asociación de un usuario a un servicio.

Tabla 16. Descripción de la verificación de un usuario en un servicio. Consulta DNS/ENUM

Número de mensaje	Descripción
1	El S-CSCF recibe en el campo R-URI un número de teléfono desde la centralita de cliente. (reenviado por el SBC)
2-3	Para poder enrutar señalización SIP es necesario obtener la SIP-URI consultando al DNS.
4	Una vez recibida la SIP-URI en el S-CSCF, se reenvía al I-CSCF para que consulte con el HSS si el usuario pertenece al servicio.
5-6-7	El I-CSCF consulta con el HSS (interfaz Cx) si el usuario pertenece al servicio solicitado y le envía la información al S-CSCF

7.9. Llamada entrante a la red de cliente desde una red externa

En el caso de que una llamada tenga como destino la IP-PABX del servicio “Conexión de grandes empresas” el número marcado correspondería a un IPrefix1. La llamada puede originarla un usuario nde la red del operador o desde otra red externa (RTB):

• Si el usuario pertenecer a la RTB, el MGC identificaría la llamada como del Servicio “Interconexión grandes clientes. El MGC consulta al DNS /ENUM por el Nº Llamado. ENUM, devuelve el valor del prefijo IPrefix2.
El MGC sustituye en la Request-URI el número destino por IPrefix1 (en ‘To’ mantiene el número).
El valor IPrefix1 lo utilizarán el CSCF y HSS para enrutar la llamada al AS del servicio.

• Si fuera desde un usuario de la Red IMS del operador, el CSCF consultará a ENUM por el número llamado yentonces ENUM le devolverá su IPrefix1.

El CSCF analizará el dominio y si es un prefijo de los que el gestiona, lanzará el 'disparo'. En caso de no gestionarlo consultará al DNS para que le devuelva la IP del CSCF que maneja IPrefix1.

Cuando el CSCF recibe el mensaje INVITE SIP, consulta el Request-URI (en este caso IPrefix1) en el HSS, y obtiene los datos de disparo hacia el AS del servicio.
obteniendo los datos para el disparo al correspondiente AS específico del Servicio (mediante el uso de un FQDN para obtener la dirección)

Una vez que el AS recibe el mensaje, analiza el parámetro Request-URI y al tratarse de un IPrefix1 realiza las siguientes funciones:

- Localiza el número que aparezca en 'To' en su lista global de usuarios.
- Incluye en el Request-URI del INVITE SIP los parámetros <Trunk Context>, <Tgrp> y 'Route' . Una vez modificado el mensaje lo reenvía al CSCF.

El CSCF que recibe la llamada envía el INVITE SIP al cluster de SBC al que pertenece el usuario destino (UA2) , como viene indicado en el 'Route' del mensaje INVITE recibido desde el AS.

El SBC, en función de los parámetros SIP "Tgrp" y "Trunk Context", encamina la petición INVITE SIP a la IP-PABX destino, o realiza funciones de Interworking si se trata de centralitas H323.

8. Conclusiones y líneas futuras de trabajo

En este apartado se pretende exponer las ideas destacables del proyecto, así como hacer una evaluación de los objetivos conseguidos y la aportación que ofrece tanto en el plano profesional como en el personal.

Como ideas principales después del estudio realizado, podemos destacar las siguientes:

- IMS es un estándar reconocido internacionalmente y especificado por los organismos 3GPP/3GPP2, ETSI y TISPAN; que define una arquitectura genérica para ofrecer servicios de VoIP y multimedia.

- La principal ventaja de la red IMS es la independencia del acceso tipo de acceso a la misma que ofrece. Basándose en los protocolos SIP e IP, es muy sencillo desarrollar servicios IMS sobre redes ya existentes.

- Para los usuarios, los servicios permiten comunicaciones usuario-usuario y usuario-contenido incluyendo voz, texto, video y múltiples combinaciones.

- Para los operadores de red, IMS introduce el concepto de arquitectura horizontal, donde la estructura, la funciones y los servicios pueden ser reusados para la nueva red, reduciendo drásticamente la inversión del operador. Además, esta arquitectura horizontal especifica interoperabilidad, '*roaming*', facturación y seguridad. Por estas razones IMS es clave para la convergencia fijo-móvil.

- En general, los operadores buscan formas rápidas y flexibles para responder a las nuevas oportunidades de negocio. Como los usuarios demandan de manera creciente servicios multimedia, los operadores quieren ser capaces de ofrecer una perfecta y coherente experiencia para el usuario con nuevos servicios accesibles e innovadores.

- Mediante el caso práctico, podemos concluir que la expansión y el aumento de la capacidad de la red IMS para el operador supone una inversión pequeña y el abanico de servicios que puede llegar a ofertar, muy elevado.

En cuanto a la aportación de este proyecto en el plano profesional, se pretende crear una guía para poder adquirir los conocimientos mínimos y necesarios a la hora de participar en el diseño de alto nivel de red de un proyecto de implementación real de la tecnología IMS, presentando de manera sencilla los nodos que forman la arquitectura principal de la red así como el funcionamiento básico de la misma.

También se presentan los conceptos del protocolo principal de la red, SIP, que serán de aplicación directa en cualquier implementación, por lo que deben ser conocidos.
Se ha presentado de manera más profunda el flujo de mensajes de señalización y datos en la fase de registro de un usuario en la red y tráfico de llamada entre usuarios de la propia red IMS porque son el pilar del conocimiento de este tipo de redes, como base para cualquier futura aplicación o interacción.

En el plano personal, se han conseguido afianzar los conceptos necesarios para desempeñar satisfactoriamente mis actividades diarias en Ericsson, ganando así seguridad en uno mismo a la vez de mejora en la coordinación, planificación, análisis y ejecución de las actividades propias de un proyecto del área IMS teniendo en cuenta que los conocimientos al inicio de mi actividad profesional en el campo de las redes de comunicaciones eran muy escasos al pertenecer al área de Sonido e Imagen dentro del ámbito de las telecomunicaciones.

A partir del trabajo elaborado en el proyecto quedan abiertas una serie de líneas futuras de trabajo, de las cuales podemos destacar el estudio en profundidad de cada uno de los nodos que integran la red, análisis de aplicaciones IMS que se implementan sobre la arquitectura básica, o el conocimiento detallado de otros protocolos que se emplean en determinadas comunicaciones de los nodos de la red.

Además, se trata de un estándar abierto en constante y rápida evolución en el que basándose en los protocolos de Internet, es posible añadir nuevas y personalizadas funcionalidades para los operadores.

Otro de los aspectos pendientes en IMS podría ser trabajar en la mejora de la calidad del servicio de la red o la capacidad que se ofrece al operador. Existirían múltiples posibilidades de ampliación, debido a que este proyecto se puede considerar una base previa al desarrollo de cualquier aplicación IMS.

9. Documentación

- Gonzalo Camarillo and Miguel A. García-Martín, “The 3G IP Multimedia Subsystem”, Wiley 2004.

- Mikka Poikselkä, Georg Mayer, Hisham Khartabil and Aki Niemi, “The IMS: IP Multimedia Concepts and Services in the Mobile Domain”, Wiley 2004.

- Alan B. Johnston, “SIP, understanding the Session Inititation Protocol”, Artech House 2004.

- Página principal del 3GPP:
  http://www.3gpp.org
  http://www.3gpp.org/specs/specs.htm (TS del 3GPP)

  3GPP TS 23228-780 IP Multimedia Subsystem (IMS);(Release 7)

  3GPP TS 23.002-720;Network architecture (Release 7)

- Página principal del IETF :
  www.ietf.org
  http://www.ietf.org/rfc.html (RFC del grupo IETF)

  - RFC 2327: SDP Session Description Protocol
  - RFC 3261: SIP Session Initiation Protocol
  - RFC 2363 : Session Initiation Protocol (SIP): Locating SIP Servers
  - RFC 3550 - RTP Transport Protocol for Real-Time Applications
  - RFC 3264: Offer/Answer Model with the Session Description Protocol (SDP)

- RFC 3372: Initiation Protocol for Telephones (SIP-T)

- Página Principal de TISPAN: http://www.etsi.org/tispan/:

- Página principal de OMA: http://www.openmobilealliance.org

- Página principal del grupo EFORT http://www.efort.com

  - Simón ZNATY, Jean-Louis DAUPHIN, Roland GELDWERTH, “IP Multimedia Subsystem : Principios y Arquitectura”, efort.

  - RTP/RTCP http://www.efort.com/media_pdf/RTP_ES_EFORT.pdf

  - Protocolo ISUP http://www.efort.com/media_pdf/ISUP_ES_EFORT.pdf

- Documentos Ericsson:

  - Call Session Control Function, 221 02-FGC 101 0266 Uen Rev A
  - MGC Description, 1551-CRA 119 456/6 Uen. 2002
  - Technical Product Description for HSS, 221 02-FGC 101 948 Uen C 2007
  - Session Border Gateway, 2/1551-HSD 101 96/1 Uen rev C 2007
  - Ericcson Withe paper 284 23 — 3001 Uen Rev C

  - IMS – IP Multimedia Subsystem, The value of using the IMS architecture, 284 23 – 3001 Uen Rev A, 2004

  - Function Specification: *SIP-H.323 Interworking*, 7/155 17-HSD 101 96/1 Uen

- Function Specification: *Media Processing*, 2/155 17-HSD 101 96/1 Uen